Ανοικτό Πανεπιστήμιο Κύπρου

Σχολή Οικονομικών Επιστημών και Διοίκησης

Πτυχιακό Πρόγραμμα Σπουδών *"Αστυνομικές Σπουδές"*

Πτυχιακή Εργασία

Dark Web: Νέα δεδομένα και προκλήσεις για τη σύγχρονη Αστυνόμευση

Μάριος Παπαϊωακείμ

Επιβλέπων Καθηγητής
Δρ. Μαρκιανός Κόκκινος

Ιούνιος 2019

Ανοικτό Πανεπιστήμιο Κύπρου

Σχολή Οικονομικών Επιστημών και Διοίκησης

Πτυχιακό Πρόγραμμα Σπουδών *"Αστυνομικές Σπουδές"*

Πτυχιακή Εργασία

Dark Web: Νέα δεδομένα και προκλήσεις για τη σύγχρονη Αστυνόμευση

Μάριος Παπαϊωακείμ

Επιβλέπων Καθηγητής
Δρ. Μαρκιανός Κόκκινος

Η παρούσα πτυχιακή εργασία υποβλήθηκε προς μερική εκπλήρωση των απαιτήσεων για απόκτηση πτυχιακού τίτλου σπουδών στο πρόγραμμα "Αστυνομικές Σπουδές" από τη Σχολή Οικονομικών Επιστημών και Διοίκησης του Ανοικτού Πανεπιστημίου Κύπρου.

Ιούνιος 2019

Περίληψη

Το διαδίκτυο είναι αποτέλεσμα της ραγδαίας ανάπτυξης της τεχνολογίας και της επιστήμης των υπολογιστών. Κατάφερε μέσα σε πολύ λίγα χρόνια να συνενώσει σχεδόν όλους τους υπολογιστές του πλανήτη και να δώσει την ευκαιρία σε αρκετούς ανθρώπους, να επικοινωνούν και να αλληλοεπιδρούν μεταξύ τους.

Την ίδια στιγμή, έδωσε απεριόριστη πρόσβαση σε μια μεγάλη και ανεξάντλητη πηγή πληροφοριών και γνώσης, που υπό διαφορετικές συνθήκες ήταν αδύνατο να συμβεί. Δεν είναι καθόλου τυχαίο το γεγονός ότι το διαδίκτυο θεωρείται από πολλούς ως ο πιο σημαντικός καταλύτης, στην πορεία για την υλοποίηση της παγκοσμιοποίησης.

Ο παγκόσμιος αυτός ιστός είναι ίσως ο μοναδικός χώρος στον οποίο δεν γίνονται διακρίσεις ως προς τους χρήστες, αφού τέτοιοι μπορεί να είναι άτομα που προέρχονται από όλες τις κοινωνικές, πολιτικές και θρησκευτικές ομάδες. Από αυτό δε θα μπορούσε να απουσιάζει ούτε και η κατηγορία εκείνη των συνανθρώπων μας που είναι επιρρεπείς στο έγκλημα.

Η παρούσα πτυχιακή μελέτη αποσκοπεί αφενός να παρουσιάσει το φαινόμενο που λέγεται διαδίκτυο και τα συστήματα εκείνα που το αποτελούν, δίνοντας περισσότερη σημασία στο αόρατο ή κρυμμένο δίκτυο (Deep Web) και σκοτεινό δίκτυο (Dark Web), αφού πρόκειται για τα μέρη εκείνα του διαδικτύου τα οποία παραμένουν κρυφά και η ύπαρξη τους είναι άγνωστη στη συντριπτική πλειοψηφία των χρηστών του. Αφετέρου, αποσκοπεί στην παρουσίαση των πιο σημαντικών κινδύνων που κρύβονται σε αυτό, καθώς επίσης παραθέτονται και μέτρα αντιμετώπισης του φαινομένου.

Summary

The internet is the outcome of the rapid technological development and computer science. Within a few years it has managed to interconnect nearly all computers on the planet and give the opportunity to all people on earth to communicate and interact.

At the same time, it has offered unlimited access to a grand and limitless source of information and knowledge, which under any other circumstances would be impossible to access. It is not by coincidence that the internet is considered to be the most important factor in the process of the materialization of globalization.

This worldwide web is most probably the unique space where there is no discrimination as far as the users are concerned, since they can derive from all social, political and religious groups. As a result, the category of people who are prone to crime could not be missing from the number of users.

The present paper is a study aiming at presenting the phenomenon of the internet and its system components, giving emphasis on the Deep Web and Dark Web; the parts that remain unknown and their existence is a secret to the majority of the internet users. On the other hand, this paper is going to present the most dangerous aspects of the internet, as well as measures of confronting and fighting this problem.

Ευχαριστίες

Με την ολοκλήρωση της πτυχιακής μου εργασίας θα ήθελα να αποδώσω θερμές ευχαριστίες στον επιβλέπων καθηγητή μου κ. Μαρκιανό Κόκκινο για την επιστημονική καθοδήγηση και την πολύτιμη, πάντα με χαμόγελο και θετική ενέργεια, βοήθειά του κατά τη συγγραφή της.

Επιπρόσθετα θα ήθελα να ευχαριστήσω και παράλληλα να αφιερώσω την πτυχιακή μου εργασία στους αφανής μου ήρωες , τη σύζυγο μου Στυλιάνα και τα δύο μου παιδιά, Αντρέα και Χριστούλλα, που μου πρόσφεραν απλόχερα όσο χρόνο χρειαζόμουν για τη συγγραφή της, ακόμα και όταν τον στερούσα από το δικό τους πολύτιμο χρόνο.

Περιεχόμενα

Κεφάλαιο 1
Εισαγωγή

Το διαδίκτυο αποτελεί ίσως την πλέον αναπτυσσόμενη και μάλιστα με γεωμετρική πρόοδο επιστήμη όλων των εποχών. Η ραγδαία ανάπτυξη του έχει επηρεάσει σε πολύ μεγάλο βαθμό ολόκληρη την ανθρωπότητα. Αρκεί κανείς να αναλογιστεί το χρόνο που χρειαζόταν να διαβιβαστεί ένα μήνυμα από μια χώρα σε μια άλλη πριν πενήντα με εκατό χρόνια, σε σχέση με τα κλάσματα του δευτερολέπτου με τα οποία ταξιδεύει τώρα η ίδια πληροφορία.

Βλέπουμε σήμερα εκατομμύρια ανθρώπους σε κάθε γωνιά της γης να εκμεταλλεύονται καθημερινά τις δυνατότητες και υπηρεσίες που παρέχει το διαδίκτυο, αφού πλέον αποτελεί την κύρια πηγή γνώσης, ενημέρωσης, ψυχαγωγίας και όχι μόνο. Σύμφωνα με τον Jeff Desjardins (2019), αυτή τη στιγμή, μέσα σε ένα μόλις λεπτό πραγματοποιούνται, 1 εκατομμύριο συνδέσεις στο Facebook, 3.8 εκατομμύρια αναζητήσεις στο Google, 4.5 εκατομμύρια προβολές βίντεο στο YouTube, στέλνονται 188 εκατομμύρια emails, ενώ εκτιμάται ότι ύψος των χρημάτων που ξοδεύονται σε online αγορές αγγίζει το $1.000.000.

Ταυτόχρονα όμως, ίσως λόγω και της ραγδαίας του ανάπτυξης, ένα μεγάλο ποσοστό αυτών των χρηστών δεν αντιλαμβάνεται τους κινδύνους που ελλοχεύουν από την αλόγιστη και ανεξέλεγκτη χρήση του. Ο άνθρωπος έχει πλέον χάσει την ιδιωτική του ζωή και η παραβίαση των προσωπικών δεδομένων του, συγκλονίζει όσο ποτέ άλλοτε. Την ίδια στιγμή, ο απλός μέσος χρήστης του διαδικτύου αδυνατεί να κατανοήσει τη λειτουργία του, πολύ περισσότερο δε, το μέγεθός του. Δεν μπορεί να διανοηθεί επίσης την ύπαρξη ενός άλλου τεράστιου διαδικτύου που λειτουργεί παράλληλα, χωρίς ωστόσο να έχει πρόσβαση σε αυτό (Jewkes & Yar, 2010).

Πρόκειται για το αόρατο ή κρυμμένο δίκτυο (Deep Web), το οποίο αναπτύχθηκε αρχικά από τις μυστικές υπηρεσίες των ΗΠΑ και αποσκοπούσε στην προστασία των πρακτόρων

τους. Βέβαια, όπως γίνεται συνήθως, η τεχνολογία δόθηκε για χρήση και στους υπόλοιπους χρήστες του διαδικτύου με σκοπό να προστατεύει την ανωνυμία και να διαφυλάσσει την ιδιωτικότητα και την ελευθερία του λόγου εκατομμυρίων χρηστών ανά το παγκόσμιο (Jewkes & Yar, 2010).

Η δυνατότητα όμως αυτή του διαδικτύου, να διατηρεί δηλαδή την ανωνυμία των χρηστών του, έτυχε πλήρης εκμετάλλευσης και από άτομα με σκοτεινές και αλλότριες προθέσεις. Έτσι, μέσα στο ίδιο το Deep Web δημιουργήθηκε το Dark Web (σκοτεινό δίκτυο), το οποίο επί της ουσίας είναι ένα υποσύστημα, η λειτουργία του οποίου περιορίζεται αποκλειστικά για τη διενέργεια παράνομων πράξεων και τη διεξαγωγή παράνομων συναλλαγών (Gehl, 2014).

Είναι πραγματικά αδιανόητο και συνάμα ασύλληπτο στον ανθρώπινο νου το τί συναντά κανείς σε αυτό το σκοτεινό δίκτυο. Ίσως η φαντασία ενός μέσου ανθρώπου να μπορέσει να προβλέψει αδικήματα όπως τη διακίνηση παιδικού πορνογραφικού υλικού και την εμπορία παράνομων λογισμικών. Κάποιοι πιο θαρραλέοι ίσως θα μπορούσαν να αναφέρουν αδικήματα όπως ξέπλυμα βρώμικου χρήματος, διακίνηση ναρκωτικών, ακόμη και δολοφονίες διάσημων προσώπων επί πληρωμή. Κι όμως στη λίστα των πιο πάνω αδικημάτων, που πραγματοποιούνται μέσα στο Dark Web, έρχεται να προστεθεί η εμπορία προσώπων και τα κυκλώματα που εμπορεύονται ανθρώπινα όργανα έναντι χρηματικού ποσού, που σε κάποιες περιπτώσεις ξεπερνά τις $200,000 (Territo & Matteson, 2011).

1.1 Σκοπός και Στόχοι

Σύμφωνα με εκτιμήσεις της γνωστής εταιρείας παροχής λογισμικού για την προστασία και ασφάλεια των Η/Υ και συστημάτων στο διαδίκτυο, Trend Micro, το ποσοστό του υλικού που είναι προσβάσιμο στο διαδίκτυο από τους απλούς χρήστες ανέρχεται μόλις στο 0,03% του παγκόσμιου ιστού. Το υπόλοιπο 99,97% αποτελείται από το Deep Web και το Dark Web (Gamer, 2015). Η πολυμορφία και οι ιδιαιτερότητες που παρουσιάζει το φαινόμενο αυτό, καθιστούν τη διερεύνηση και δίωξή του σχεδόν αδύνατη, αφού η οποιαδήποτε επικοινωνία ή συναλλαγή πραγματοποιείται σε αυτό, γίνεται στον υψηλότερο βαθμό κρυπτογράφησης και ασφάλειας, ο εντοπισμός του δε, θεωρείται ιδιαίτερα δύσκολος έως και αδύνατος.

Οι πιο πάνω λόγοι, υπήρξαν η βασικότερη αιτία για τη συγγραφή της παρούσας πτυχιακής εργασίας, που σκοπό έχει να καταγράψει αφενός τους κινδύνους που ελλοχεύουν μέσα από τη χρήση του σκοτεινού δικτύου και αφετέρου, να παρουσιάσει τους τρόπους αντιμετώπισης και χειρισμού του από τις αρχές επιβολής του νόμου.

Βασικός στόχος της παρούσας εργασίας είναι να επεξηγήσει τον τρόπο λειτουργίας του διαδικτύου και κατ' επέκταση να διαχωρίσει το ρόλο και την λειτουργία του Deep Web και του Dark Web. Επιπρόσθετα, να παρουσιάσει τις διάφορες εγκληματικές δράσεις που λαμβάνουν χώρα μέσα στα σκοτεινά και απόκρυφα μέρη του παγκόσμιου ιστού (Dark Web) και πως αυτές επηρεάζουν την ευρύτερη κοινωνία, οικονομία, καθώς και άλλους τομείς.

Τέλος, τα ευρήματα της παρούσας εργασίας αναμένεται να αποτελέσουν μια σημαντική αναφορά για τις διωκτικές αρχές και την Αστυνομία Κύπρου για κατανόηση του φαινομένου, των παράνομων δραστηριοτήτων που συνδέονται με αυτό, των δραστών που κρύβονται σε αυτό και τα σύγχρονα εγκλήματα που αναδύονται από αυτό, καθώς και οι διάφοροι τρόποι χειρισμού και αντιμετώπισης του.

1.2. Μεθοδολογία Έρευνας

Για την εκπόνηση της εν λόγω διπλωματικής εργασίας χρησιμοποιήθηκε υλικό από πηγές όπως δημοσιεύματα, καθώς και εγχειρίδια που εκδίδονται προς τους πολίτες. Παράλληλα βασίστηκε στη βιβλιογραφική ανασκόπηση σε βιβλία και εγχώριες και διεθνείς κυρίως μελέτες που αφορούν το Dark Web. Συγκεκριμένα, μελετήθηκαν βιβλία δημοσιεύσεις σε επιστημονικά περιοδικά που αφορούν τον τρόπο λειτουργίας του διαδικτύου και Deep Web, το φαινόμενο Dark Web με σκοπό την κατανόησή του και το πώς αυτό εξελίχθηκε μέχρι σήμερα. Επίσης, αξιοποιήθηκαν πηγές που αφορούν την επικρατούσα κατάσταση σε ευρωπαϊκό αλλά και παγκόσμιο επίπεδο και μελετήθηκαν βέλτιστες πρακτικές που εφαρμόζονται για την πρόληψη και αντιμετώπιση του φαινομένου.

Η παρούσα εργασία αποτελείται από επτά κεφάλαια, συμπεριλαμβανομένου του πρώτου που είναι η εισαγωγή. Στο δεύτερο κεφάλαιο, γίνεται μία ιστορική αναδρομή του διαδικτύου και πως αυτό εξελίχθηκε στη σημερινή του μορφή. Το τρίτο κεφάλαιο αφορά την ύπαρξη του κρυφού ή αόρατου δικτύου (Deep Web και το παρουσιάζεται το περιεχόμενο αλλά και οι διαφορές του με το συμβατικό δίκτυο. Στο επόμενο κεφάλαιο,

παρουσιάζεται το σκοτεινό δίκτυο (Dark Web), ο τρόπος λειτουργίας του, τα εργαλεία και το νόμισμα που χρησιμοποιείται για την τέλεση των διαφόρων συναλλαγών μέσα σε αυτό και οι σημαντικές διαφορές του με το Deep Web.

Το πέμπτο κεφάλαιο παρουσιάζει τις κατηγορίες των παράνομων δραστηριοτήτων που πραγματοποιούνται μέσα από το Dark Web, καθώς επίσης τους κινδύνους που ελλοχεύουν για τον απλό χρήστη και τα πιο συχνά εγκλήματα που λαμβάνουν χώρα σε αυτό. Στο τελευταίο κεφαλαίο πριν τον επίλογο γίνονται εισηγήσεις για τρόπους αντιμετώπισης του φαινομένου από τις διωκτικές αρχές αλλά και από τους απλούς πολίτες, αφού η συνεργασία θεωρείται επιβεβλημένη, προκειμένου να επέλθει μείωση του φαινομένου αυτού.

1.3 Περιορισμοί και Δυσκολίες

Σημαντικός περιορισμός για τη συγγραφή της εν λόγω διπλωματικής εργασίας αποτέλεσε το γεγονός ότι πρόκειται για ένα σχετικά νέο φαινόμενο το οποίο βρήκε απροετοίμαστη τόσο την ακαδημαϊκή κοινότητα, όσο και την ευρύτερη κοινωνία. Για την ακρίβεια, η επιστημονική κοινότητα ασχολήθηκε με το Dark Web τα τελευταία δέκα με δεκαπέντε χρόνια, αφού εκ των πραγμάτων η γένεσή του τοποθετείται χρονικά στην δεκαετία του '90, οι πρώτες δε περιπτώσεις που απασχόλησαν τις αρχές, καταγράφονται στις αρχές του 21ου αιώνα. Τα σχετικά στατιστικά στοιχεία είναι πολύ περιορισμένα για να εκτιμηθεί το μέγεθος του προβλήματος και συνεπώς οι οποιεσδήποτε αναφορές σε αριθμητικά δεδομένα είναι απλά εκτιμήσεις. Τέλος, η συλλογή πληροφοριών και στοιχείων για την παρουσία του φαινομένου στην Κύπρο είναι από μηδαμινή έως ανύπαρκτη.

Κεφάλαιο 2
Η ιστορία του Διαδικτύου

Το διαδίκτυο είναι ένα παγκόσμιο δίκτυο που αποτελείται από πολλά άλλα δίκτυα ηλεκτρονικών υπολογιστών. Επί της ουσίας, πρόκειται για ένα πλέγμα από εκατομμύρια ηλεκτρονικών υπολογιστών που είναι διασυνδεμένοι μεταξύ τους σε κάθε γωνιά του πλανήτη. Τι ήταν όμως αυτό που πυροδότησε αυτή τη συστημική ανάπτυξη;

2.1 Ένα ενδιαφέρον πείραμα ξεκινά

Το διαδίκτυο, αποτελεί απόγονο του Αμερικανικού Πενταγώνου. Αφορμή για τη δημιουργία του αποτέλεσε το γεγονός ότι κατά τη διάρκεια του ψυχρού πολέμου, το 1957, η πρώην Ένωση Σοβιετικών Σοσιαλιστικών Δημοκρατιών (ΕΣΣΔ) είχε ήδη στείλει στο διάστημα τον πρώτο δορυφόρο της. Αυτό προκάλεσε φόβο στο αμερικανικό υπουργείο άμυνας, το οποίο αντέδρασε με την ίδρυση της Υπηρεσίας Προηγμένων Ερευνητικών Προγραμμάτων ARPA (Advanced Research Project Agency). Κύρια αποστολή της εν λόγω υπηρεσίας ήταν να βοηθήσει τις στρατιωτικές δυνάμεις των ΗΠΑ να αναπτυχθούν τεχνολογικά και να δημιουργηθεί ένα δίκτυο επικοινωνίας το οποίο θα εξασφάλιζε την επικοινωνία μεταξύ απομακρυσμένων δικτύων και θα μπορούσε να επιβιώσει σε μια ενδεχόμενη πυρηνική επίθεση (Jewkes & Yar, 2010).

2.1.1 Δεκαετία '60: Η γένεσίς

Στα πλαίσια λοιπόν του προγράμματος ARPA, το 1969, δημιουργήθηκε αρχικά ένα δίκτυο που συνέδεε τέσσερις υπερ-υπολογιστές. Ο ένας ήταν εγκατεστημένος στο Πανεπιστήμιο της California στο Los Angeles (UCLA), ο άλλος στο Πανεπιστήμιο της Santa Barbara, ο τρίτος στο Πανεπιστήμιο Utah και ο τέταρτος στο Ινστιτούτο Ερευνών του Stanford (Zimmermann & Emspak, 2017).

Το δίκτυο αυτό έμεινε γνωστό στην ιστορία ως ARPANET, και ήταν κατασκευασμένο με τέτοιον τρόπο, ώστε αν για κάποιον λόγο ένα τμήμα του έβγαινε εκτός λειτουργίας, το υπόλοιπο να λειτουργεί χωρίς προβλήματα (Πανεπιστήμιο Θεσσαλίας, 1997).

Έτσι λοιπόν, σε αρχικό στάδιο επέτρεπε σε υπολογιστές από τα τέσσερα πανεπιστήμια να μοιράζονται δεδομένα και ταυτόχρονα στους ερευνητές να χρησιμοποιήσουν για πρώτη φορά τον πρόγονο του σημερινού ηλεκτρονικού ταχυδρομείου (Zimmermann & Emspak, 2017).

2.1.2 Δεκαετία '70: Οι πρώτες συνδέσεις

Προκειμένου να ξεπεραστούν οι διαφορετικοί τρόποι επικοινωνίας που χρησιμοποιούσε κάθε δίκτυο για να διακινεί τα δεδομένα του, αλλά και να επιλυθούν και να καθοριστούν πρωτόκολλα επικοινωνίας μεταξύ των διαφόρων δικτύων, το 1973, ξεκινά ένα νέο ερευνητικό πρόγραμμα που ονομάζεται Internetting Project (Internet Society, 2019). Μέσα από αυτό, προκύπτει το γνωστό πλέον σε όλους πρωτόκολλο IP, με το οποίο οι διάφοροι Ηλεκτρονικοί υπολογιστές (Η/Υ) μπορούν να συνδέονται και να αποτελούν ένα διαδίκτυο. Σε ένα δίκτυο IP όλοι οι υπολογιστές είναι ισοδύναμοι, καθιστώντας ικανό οποιονδήποτε υπολογιστή του διαδικτύου να μπορεί να επικοινωνεί με οποιονδήποτε άλλον (Zimmermann & Emspak, 2017).

Την ίδια περίοδο, στα πλαίσια του πιο πάνω προγράμματος, καθιερώνεται μια άλλη τεχνική που αποσκοπεί στον έλεγχο της μετάδοσης των δεδομένων, το Transmission Control Protocol (TCP) (Πρωτόκολλο Ελέγχου Μετάδοσης). Επίσης, ορίζονται προδιαγραφές για τη μεταφορά αρχείων μεταξύ υπολογιστών (FTP) και το βελτιωμένο πρωτόκολλο ηλεκτρονικού ταχυδρομείου (E-mail) (Πανεπιστήμιο Θεσσαλίας, 1997).

Επίσης, σταδιακά, συνδέονται με το ARPANET ιδρύματα από άλλες χώρες, με πρώτα το University College of London (Αγγλία) και το Royal Radar Establishment (Νορβηγία) (Πανεπιστήμιο Θεσσαλίας, 1997).

2.1.3 Δεκαετία '80: Ένα παγκόσμιο δίκτυο για την ακαδημαϊκή κοινότητα

Το 1983, θα μπορούσε να χαρακτηριστεί και ως έτος σταθμός στην ιστορία του Internet, αφού το πρωτόκολλο TCP/IP (δηλ. ο συνδυασμός των TCP και IP) αφενός αναγνωρίζεται ως πρότυπο από το Υπουργείο Άμυνας των ΗΠΑ, αφετέρου, αποτελεί το βασικό πρωτόκολλο επικοινωνίας όλου του παγκόσμιου ιστού μέχρι και σήμερα (Blank, 2002, σσ. 9-10).

Στην ευρεία διάδοσή του, σημαντικό ρόλο διαδραμάτισε και η ενσωμάτωση του στο λειτουργικό σύστημα Berkeley UNIX, το οποίο ήταν το πιο διαδεδομένο την συγκεκριμένη περίοδο. Έτσι, μέσα σε ελάχιστο χρόνο, εκατοντάδες Πανεπιστήμια κατάφεραν να συνδέουν τους υπολογιστές τους στο ARPANET, το οποίο όμως επιβαρύνεται πολύ και έτσι το 1983, διαχωρίζεται σε δύο τμήματα. Συγκεκριμένα στο MILNET (για αυστηρά στρατιωτικές επικοινωνίες) και στο νέο ARPANET (για χρήση αποκλειστικά από την πανεπιστημιακή κοινότητα και συνέχιση της έρευνας στη δικτύωση) (Πανεπιστήμιο Θεσσαλίας, 1997).

Το 1985, το National Science Foundation (NSF) δημιουργεί το δικό του γρήγορο δίκτυο, το NSFNET, το οποίο όμως για σκοπούς συμβατικότητας χρησιμοποιεί επίσης το πρωτόκολλο TCP/IP. Σκοπός της δημιουργίας του η σύνδεση των υφιστάμενων υπέρ-υπολογιστών με την υπόλοιπη επιστημονική κοινότητα. Σε αυτό συνδέονται αρκετές χώρες μεταξύ των οποίων ο Καναδάς, Γαλλία, Σουηδία, Αυστραλία, Γερμανία, Ιταλία, κ.α. (Πανεπιστήμιο Θεσσαλίας, 1997)

2.1.4 Δεκαετία '90: Ένα παγκόσμιο δίκτυο για όλους

Την επόμενη δεκαετία, όλο και περισσότερες χώρες συνδέονται στο NSFNET, μεταξύ των οποίων και η Ελλάδα το 1990.

Το 1993, στο εργαστήριο CERN στην Ελβετία, ο Tim Berners-Lee παρουσιάζει επίσημα για πρώτη φορά το World Wide Web (WWW). Πρόκειται για ένα σύστημα διασύνδεσης πληροφοριών σε μορφή πολυμέσων που βρίσκονται αποθηκευμένες σε χιλιάδες υπολογιστές του Internet σε ολόκληρο τον κόσμο και παρουσίασής τους σε ηλεκτρονικές σελίδες. Το γραφικό αυτό περιβάλλον έκανε την εξερεύνηση του Internet προσιτή στον απλό χρήστη (CERN, 2019).

2.2 Τρόπος λειτουργίας του Διαδικτύου

Το Internet δεν είναι ένα απλό δίκτυο, αλλά ένα διαδίκτυο. Χρειάζεται επομένως ένα σύνολο από συμβάσεις που να καθορίζουν το πως ανταλλάσσουν μεταξύ τους δεδομένα οι υπολογιστές που μπορεί να είναι διαφορετικού τύπου και να ανήκουν σε διαφορετικά δίκτυα.

Ακριβώς αυτό το σύνολο συμβάσεων προσφέρει το TCP/IP. Όλοι οι υπολογιστές που είναι συνδεδεμένοι στα χιλιάδες μικρότερα δίκτυα του Internet τρέχουν το πρωτόκολλο TCP/IP και έτσι μιλούν μια κοινή γλώσσα που τους επιτρέπει να «συνεννοούνται» παρά τις διαφορές τους (Blank, 2002).

2.2.1 Τρόποι πρόσβασης

Για να καταστεί εφικτή λοιπόν η επικοινωνία όλων αυτών των Η/Υ, θα πρέπει στον κάθε Η/Υ να αντιστοιχεί και μία μοναδική διεύθυνση η οποία καλείται IP και στην ουσία αποτελεί τη μοναδική ταυτότητα του συγκεκριμένου υπολογιστή στο διαδίκτυο.

Η διεύθυνση IP ή αλλιώς IPv4 όπως επικράτησε σήμερα, χρησιμοποιεί διευθύνσεις 32bit, οι οποίες περιορίζουν το ποσό των διευθύνσεων στα 4 δισεκατομμύρια. Κάθε διεύθυνση IPv4 έχει τέσσερα bytes, καθένα από τα οποία έχει μέγιστη τιμή 255. Μία διεύθυνση IPv4 έχει τη μορφή XXX.XXX.XXX.XXX (Blank, 2002, σσ. 66-74).

Σήμερα, λόγω του προβλήματος της έλλειψης επαρκών διευθύνσεων IPv4, η IETF (Internet Engineering Task Force) ανέπτυξε το πρωτόκολλο IPv6. Το IETF είναι ένας οργανισμός ανοιχτού τύπου που αναπτύσσει και προωθεί τα πρότυπα διαδικτύου, ειδικά στη βάση του TCP/IP. Το IPv6 προορίζεται τα επόμενα χρόνια να αντικαταστήσει το IPv4 (Blank, 2002, σσ. 202-206)

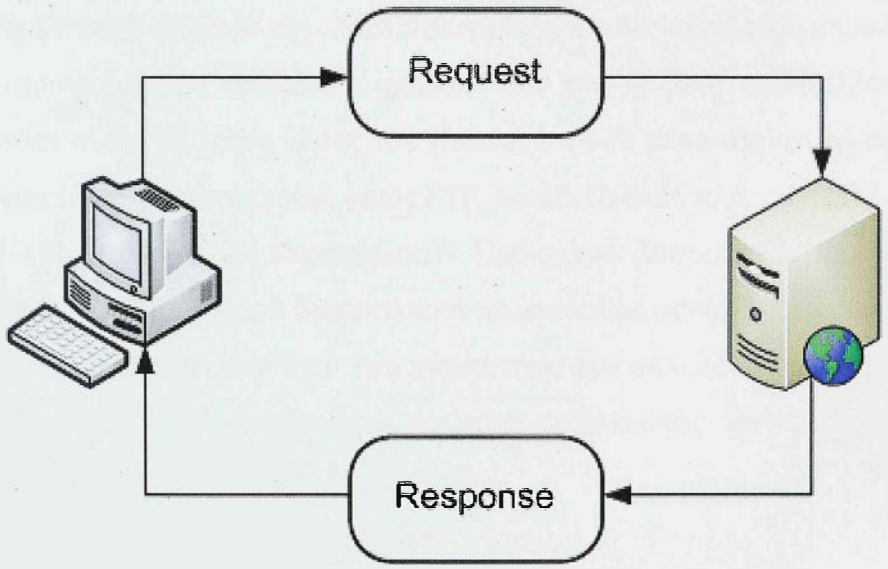
Λόγω όμως του τεράστιου αριθμού συνδεδεμένων Η/Υ και συστημάτων η αποστήθιση μιας τέτοιας διεύθυνσης είναι πρακτικά αδύνατη, έχει χρησιμοποιηθεί η τεχνικής της ονοματοδοσίας των υπολογιστών μέσω μίας μεθόδου που ονομάζεται DNS (Domain Name System). Με αυτή την πρακτική λύση, έχουμε σήμερα τις γνωστές σε όλους και ευανάγνωστες διευθύνσεις ιστοσελίδων. Για παράδειγμα για την ιστοσελίδα στην οποία

βρίσκεται η γνωστή μηχανή αναζήτησης της Google, η www.google.com, ο υπεύθυνος DNS αναλαμβάνει την μετάφραση στη διεύθυνση IP 172.217.16.132 (Blank, 2002, σ. 75).

Μία δεκαετία αργότερα, το 1998, ιδρύεται στις Η.Π.Α. μια μη κερδοσκοπική εταιρία δημοσίου συμφέροντος, το ICANN (Internet Corporation for Assigned Names and Numbers), με συμμετέχοντες από όλο τον κόσμο που σκοπό έχουν τη διατήρηση ενός ασφαλούς, σταθερού και λειτουργικού Διαδικτύου. Μια από τις κύριες αποστολές της η ανάπτυξη πολιτικής και η καθιέρωση των μοναδικών αναγνωριστικών χαρακτηριστικών του Διαδικτύου. Επίσης, μέσω της συνεργασίας της με το σύστημα ονοματοδοσίας του Διαδικτύου (DNS), διαδραματίζει σημαντικό ρόλο στην επέκταση και εξέλιξη του Διαδικτύου (ICANN, 2019).

2.2.2 Το μοντέλο πελάτη – εξυπηρετητή

Το βασικό μοντέλο πάνω στο οποίο στηρίζεται η όλη φιλοσοφία του Internet ονομάζεται "Client-Server" ή στα ελληνικά μοντέλο πελάτη – εξυπηρετητή. Προκειμένου να επιτευχθεί μία σύνδεση και να ανακτηθεί η απαιτούμενη από το χρήστη πληροφορία, θα πρέπει ο χρήστης ή αλλιώς πελάτης (Client) αρχικά να ζητήσει από την πλευρά του πρόσβαση και προβολή δεδομένων από συγκεκριμένη ιστοσελίδα, π.χ. να διαβάσει μια διαδικτυακή εφημερίδα. Ακολούθως, ο εξυπηρετητής (Server) από την πλευρά του, αφού κατανοήσει και αποκωδικοποιήσει σωστά το αίτημα του χρήστη, προβαίνει στην ανάκτηση των πληροφοριών από τη βάση δεδομένων του και στην συνέχεια τα τροχιοδρομεί πίσω στον αιτητή.



Εικόνα 1: Επεξήγηση του τρόπου λειτουργίας του μοντέλου Client-Server

2.2.3 Οι κυριότερες υπηρεσίες του διαδικτύου στη σύγχρονη εποχή

Όπως ήταν αναμενόμενο, η αρχική μορφή και δυνατότητες του internet έχουν εξελιχθεί, έτσι ώστε να καλύπτουν μια ευρεία θεματολογία και τομείς υπηρεσιών. Μερικές από αυτές τις υπηρεσίες είναι:

- **Email (Ηλεκτρονικό ταχυδρομείο):** αποσκοπεί στην ανταλλαγή μηνυμάτων μεταξύ χρηστών, κάνοντας χρήση της προσωπικής ηλεκτρονικής διεύθυνσης που ο κάθε ένας διαθέτει. Το περιεχόμενο πλέον μπορεί να αποτελείτε από απλό κείμενο, φωτογραφίες, βίντεο, ή ακόμη και ολόκληρη βάση δεδομένων.
- **Mailing List (Λίστες Email):** αξιοποιεί τις δυνατότητες της προηγούμενης με τη διαφορά ότι απευθύνεται σε περιορισμένο αριθμό χρηστών, ελεγχόμενο από κάποιο διαχειριστή και σκοπό έχει την ανταλλαγή πληροφοριών ή γνώσης ανάμεσα στα μέλη της ομάδας.
- **Usenet:** Κάτι παρόμοιο με το προηγούμενο, αφού επιτρέπει την ανταλλαγή μηνυμάτων σε ομάδες συζητήσεων σε μία ευρεία γκάμα θεμάτων σε παγκόσμιο επίπεδο.
- **FTP (File Transfer Protocol):** Κάνει ότι ακριβώς λέει ο τίτλος του, δηλαδή ρυθμίζει και επιτρέπει τη μεταφορά αρχείων από ένα τοπικό υπολογιστή σε κάποιο απομακρυσμένο υπολογιστή, ο οποίος μπορεί να είναι σε οποιοδήποτε άλλο μέρος του κόσμου.
- **Chat / Talk:** Ίσως η πιο διαδεδομένη πλέον υπηρεσία στις μέρες μας, αφού επιτρέπει την ανταλλαγή μηνυμάτων κειμένου σε πραγματικό χρόνο μεταξύ δύο ή περισσότερων χρηστών που βρίσκονται σε απομακρυσμένα σημεία.
- **WWW (World Wide Web):** Αναφέρεται στις διαδικτυακές ηλεκτρονικές σελίδες με πληροφορίες σε γραφικό - φιλικό προς τον χρήστη περιβάλλον. Το WWW αποτελεί το μεγαλύτερο μέρος του Internet, αφού μέσα από αυτό συνδυάζονται και αρκετές άλλες υπηρεσίας όπως FTP, Email, Usenet, κλπ.
- **MUD (Multiple User Dimension):** Πρόκειται βασικά για μια νέα σχετικά υπηρεσία, η οποία αφορά διαδικτυακά παιχνίδια με σενάριο στα οποία ο χρήστης συνδέεται, φτιάχνει τον δικό του χαρακτήρα και αλληλοεπιδρά στο περιβάλλον και την πλοκή του παιχνιδιού με τους υπόλοιπους παίκτες (Πανεπιστήμιο Θεσσαλίας, 1997).

Βέβαια, η επόμενη μορφή υπηρεσιών διαδικτύου, στην οποία έχουμε ήδη εισέλθει, είναι αυτή του Ίντερνετ των πραγμάτων (IoT: Internet of Things) και το Internet όλων (IoE: Internet of Everything). Συγκεκριμένα ο όρος :

- **IoT** – αφορά στην επικοινωνία μεταξύ μηχανών, όπου πρόκειται για φυσικές συσκευές που διαθέτουν αισθητήρες και μπορούν να συνδεθούν στο διαδίκτυο, επομένως να ανταλλάξουν δεδομένα. Ένα παράδειγμα είναι ένα έξυπνο ρολόι πολλαπλών σπορ που διαβάζει πληροφορίες από τη ζώνη παλμών όταν ο χρήστης αθλείται και αποθηκεύει όλα τα δεδομένα κατά τη διάρκεια της άσκησης. Όταν ολοκληρώσει τη άσκηση, μεταφέρει τα δεδομένα σε μια εφαρμογή στο smartphone και τα αξιοποιεί αναλόγως (Kellmereit & Obodovski, 2013, σσ. 13-20).
- **IoE** – αφορά την επικοινωνία μεταξύ ανθρώπων (χρήστες) και μηχανών, το γνωστό έξυπνο σπίτι. Ένα παράδειγμα είναι ένας αισθητήρας σε ένα κάδο απορριμμάτων. Όταν το επίπεδο απορριμμάτων φτάσει σχεδόν γεμάτο, ο αισθητήρας στέλνει ένα μήνυμα σε ένα smartphone ότι πρέπει να αδειάσει το σκουπιδοτενεκέ (Batalla, Mastorakis, Mavromoustakis, & Pallis, 2017, σσ. 5-7).

2.2.4 Βασικά χαρακτηριστικά του Διαδικτύου

Πέραν της μαγείας που προσφέρει το διαδίκτυο μέσα από την ανεξίτηλη πηγή γνώσεων, ψυχαγωγίας και αλληλεπίδρασης ανθρώπου και μηχανής, αυτό που το κάνει ιδιαίτερα σημαντικό και ταυτόχρονα δελεαστικό είναι το γεγονός ότι από τη δεκαετία του '90 και έπειτα, περίοδο κατά την οποία διαχωρίστηκε από το ARPANET, παρέμεινε ένα αποκεντρωμένο και αυτό-διαχειριζόμενο δίκτυο.

Αυτό δηλαδή σημαίνει ότι, δεν υπάρχει κάποιος κεντρικός φορέας ή οργανισμός που α) να το διευθύνει, β) να το χαλιναγωγεί και γ) να παίρνει συνολικά αποφάσεις σχετικά με το είδος των πληροφοριών που διακινούνται, τις υπηρεσίες που παρέχονται από τους διάφορους υπολογιστές του ή τη διαχείρισή του.

Έκτοτε, καθιερώθηκε η θεμελιώδης αρχή της ουδετερότητας στο Διαδίκτυο, που σημαίνει ότι, η πρόσβαση σε όλες τις ιστοσελίδες και τις διαδικτυακές υπηρεσίες θα πρέπει να είναι ίση απέναντι σε όλους και να μην καταλαμβάνεται από διακρίσεις με βάση το χρήστη, το περιεχόμενο ή την πλατφόρμα . (Mueller, 2010).

Εξασφαλίζει, δηλαδή, σε κάθε άνθρωπο τη δυνατότητα να δημιουργεί τη δική του ιστοσελίδα/υπηρεσία και να παρέχει ελεύθερη πρόσβαση σε αυτήν (Strickland, 2008).

Χωρίς την εν λόγω αρχή, ο εκάστοτε πάροχος υπηρεσιών διαδικτύου (ISP) θα μπορούσε να υποβαθμίζει ή να περιορίζει εσκεμμένα τη δυνατότητα πρόσβασης σε συγκεκριμένες ιστοσελίδες/υπηρεσίες ή να επιβάλλει επιπλέον χρεώσεις για την πρόσβαση σε αυτές. Επίσης, θα μπορούσε να μπλοκάρει αυθαίρετα οποιαδήποτε ιστοσελίδα στην οποία δεν επιθυμεί να έχουν πρόσβαση οι χρήστες, όπως για παράδειγμα τυχόν ανταγωνιστικές ιστοσελίδες/υπηρεσίες. Τέτοια φαινόμενα βέβαια παρατηρούνται σε δικτατορικά καθεστώτα, όπως την Τουρκία ή την Βόρεια Κορέα (Mueller, 2010, σσ. 16-17)

Κεφάλαιο 3
Deep Web: ορισμός και χαρακτηριστικά

Τον όρο Deep Web (επίσης γνωστό και ως Deepnet, Undernet, στην ελληνική το αόρατο ή κρυμμένο δίκτυο) επινόησε ο ιδρυτής του BrightPlanet, Mike Bergman και αναφέρεται στο περιεχόμενο του διαδικτύου που δεν ανήκει στο συμβατικό ή επιφανειακό Web (Surface Web) και ούτε μπορεί να εντοπιστεί και να καταγραφεί από το ευρετήριο μίας συνηθισμένης μηχανής αναζήτησης (Bergman, 2001).

Στην προσπάθεια του να επεξηγήσει και να αποδώσει την ερμηνεία του όρου, παρομοίασε το χρήστη σαν ένα ψαρά ο οποίος σέρνει ένα δίκτυ στην επιφάνεια του ωκεανού. Σίγουρα θα πιαστούν αρκετά ψάρια στο δίκτυ του, αλλά σε καμία περίπτωση δεν θα κατορθώσει να πάρει όλο εκείνο τον πλούτο που βρίσκεται κρυμμένος στα βαθιά (Bergman, 2001).

3.1 Περιγραφή

Όπως αναφέρθηκε προηγουμένως στην εισαγωγή, υπάρχει μια τεράστια, εξίσου σημαντική ζωή κάτω από την επιφάνεια του συμβατικού Web. Αυτό το τμήμα του διαδικτύου δεν είναι ευρετηριασμένο - δεν μπορεί δηλαδή να προσεγγιστεί με κανονικούς περιηγητές ιστού - όπως το Edge, το Firefox, το Safari και το Opera. Ωστόσο, αν γνωρίζει κανείς πως να φτάσει σε αυτό, εκεί θα βρει μια πλειάδα από ακαδημαϊκές και όχι μόνο βάσεις δεδομένων, ιατρικά και οικονομικά αρχεία, νομικά έγγραφα, επιστημονικές αναφορές ή/και μετρήσεις, κυβερνητικές εκθέσεις, συνδρομητικές υπηρεσίες κ.λπ., καθώς και το λεγόμενο Dark Web (Pederson, 2016).

Σύμφωνα με σχετική έκθεση αξιολόγησης του σοβαρού και οργανωμένου εγκλήματος εντός της Ευρωπαϊκής Ένωσης, διαφαίνεται ότι τον Ιανουάριο του 2017, ο αριθμός των χρηστών του εν λόγω δικτύου ξεπερνούσε τα 1.7 εκατομμύρια, έχοντας στη διάθεσή τους

πέραν των 60,000 μοναδικών ιστοσελίδων (SOCTA, 2017). Αυτή τη στιγμή, ο αριθμός των χρηστών ξεπερνά τα 2.5 εκατομμύρια και ο αριθμός των ιστοσελίδων τις 85.000 (Tor Metrics, 2019).

Για να καταστεί αντιληπτό το μέγεθος του Deep Web, χαρακτηριστική είναι η γνωστή πλέον εικόνα του παγόβουνου που κυκλοφορά στους διάφορους διαδικτυακούς χώρους, όπου γίνεται αναφορά για το Deep και Dark Web (Bergman, 2001).

Το παράδοξο με το Deep Web είναι ότι, ενώ είναι εύκολο να γίνει αντιληπτό γιατί είναι υπαρκτό, είναι πολύ δύσκολο να προσδιοριστεί με συγκεκριμένους όρους η λειτουργία του. Με λίγα λόγια, το Deep Web, αποτελείται από περιεχόμενο που έχει αποκλειστεί από μηχανές αναζήτησης γενικής χρήσης όπως οι Google, Bing και Yahoo. Δεν υπάρχει τίποτα εγγενώς "αόρατο" για αυτό το περιεχόμενο. Αλλά επειδή αυτό το περιεχόμενο δεν είναι εύκολα ανιχνεύσιμο από τα εργαλεία αναζήτησης πληροφοριών (Search Engines) που χρησιμοποιούνται από τους περισσότερους χρήστες του Διαδικτύου, είναι πραγματικά αόρατο επειδή είναι όντως δύσκολο να εντοπιστεί αν δεν ξέρει κάποιος ακριβώς πού να το ψάξει (Price & Sherman, 2001).

3.2 Συμβατικό vs Deep Web

Διάφορες μελέτες που έχουν γίνει τα τελευταία χρόνια, επιβεβαιώνουν τις προαναφερθείσες εκτιμήσεις της Trend Micron. Χαρακτηριστικά ο CEO της BrightPlanet, Steve Pederson, αναφέρει ότι, το μέγεθος του Deep Web είναι έως και 400-500 φορές μεγαλύτερο από αυτό του συμβατικού δικτύου και καταλαμβάνει γύρω στο 96% του περιεχομένου του διαδικτύου (Bergman, 2001).

Σε μια άλλη έρευνα, αυτή των Murray και Moen (2015), προκύπτει ότι, ο αριθμός των συνδέσεων του παγκόσμιου ιστού οι οποίες αντιστοιχούν στο Deep Web παρουσιάζουν πολύ μεγάλο ρυθμό αύξησης. Το φαινόμενο αυτό κρίνεται ιδιαίτερα ανησυχητικό, καθώς έχει ήδη καταγραφεί η τάση μετατόπισης του "παραδοσιακού" εγκλήματος στον ψηφιακό κόσμο.

Επιπλέον, σύμφωνα με διάφορες μετρήσεις της ιστοσελίδας DeepWeb-Sites.com (2019), οι οποίες συγκρίνουν το Deep Web με το συμβατικό ή δημόσιο δίκτυο, προκύπτουν τα ακόλουθα ενδιαφέροντα στοιχεία, το Deep Web περιέχει 7,500 terabytes πληροφορίες σε

αντίθεση με το συμβατικό που έχει μόλις 19 terabytes. Το Deep Web περιέχει περίπου 500 δισεκατομμύρια διαφορετικά αρχεία, ενώ το συμβατικό έχει μόλις 1 δισεκατομμύριο. Παρόλο που οι σελίδες του Deep Web δεν είναι ευρέως γνωστές, ούτε εντοπίζονται από τις διάφορες μηχανές αναζήτησης, εντούτοις, κατά μέσο όρο, δέχονται μηνιαία 50% περισσότερους επισκέπτες και είναι πιο ισχυρά συνδεδεμένες με άλλες σελίδες σε σύγκριση με αυτές του συμβατικού δικτύου. Επιπρόσθετα, οι ιστοσελίδες του Deep Web, τείνουν να είναι μικρότερες σε έκταση με βαθύτερο και ποιοτικότερο όμως περιεχόμενο (1000-2000 φορές μεγαλύτερο από το αντίστοιχο συμβατικό) και το περιεχόμενο τους τείνει να είναι αρκετά πιο σχετικό και ακριβές με την πληροφορία που ψάχνει ο χρήστης, σε σύγκριση με το συμβατικό το οποίο στις πλείστες των περιπτώσεων οι μηχανές αναζήτησης παρουσιάζουν και αποτελέσματα, τελείως άσχετα με την αναζήτηση.

Στο συμβατικό δίκτυο, το περιεχόμενο των διαφόρων ιστοσελίδων ανακτάται και κατηγοριοποιείται από τις μηχανές αναζήτησης με βάση τους διάφορους συνδέσμους που βρίσκονται σε αυτές. Ο βασικός λόγος για τον οποίο τα αποτελέσματα που προκύπτουν από αναζητήσεις σε αυτό είναι ανεπαρκή, είναι το γεγονός ότι οι μηχανές αναζήτησης αδυνατούν αφενός να συμπεριλάβουν δυναμικό περιεχόμενο στις βάσεις τους, αφετέρου, δεν έχουν την ικανότητα να σκεφτούν, οπότε μηχανικά ακολουθούν τους συνδέσμους και τις πληροφορίες που τους αφορούν (Lautenschlager, 2016).

Αντιθέτως, το Deep Web λειτουργεί με ένα εντελώς διαφορετικό τρόπο, τοποθετεί το μεγαλύτερο μέρος των εγγράφων και των πληροφοριών που περιέχονται σε αυτά σε περιορισμένης πρόσβασης βάσεις δεδομένων. Έτσι στον κάθε χρήστη, παρέχεται αποκλειστικά και μόνο το συγκεκριμένο και συνήθως εξειδικευμένο περιεχόμενο το οποίο αιτείται (Lautenschlager, 2016).

3.3 Μηχανές αναζήτησης και Deep Web

Όπως έχει προαναφερθεί, η δεκαετία του '90 αποτέλεσε σταθμό για την ανάπτυξη του διαδικτύου. Παρόλο που αρχικά ξεκίνησε με ένα πολύ μικρό και ελεγχόμενο αριθμό ιστοσελίδων, πολύ σύντομα γνώρισε τεράστια ανάπτυξη σε βαθμό που η δημιουργία ενός ευρετηρίου κατέστη επιτακτική ανάγκη. Έτσι, το 1994, ξεκίνησε την λειτουργία της η πρώτη μηχανή αναζήτησης, η Lycos, η οποία περιλάμβανε μόλις 54,000 έγγραφα στη βάση της (Zilman, 2019).

Στα αμέσως επόμενα χρόνια και συγκεκριμένα το 1996, τα δεδομένα αλλάζουν άρδην την μορφή και το χαρακτήρα του διαδικτύου αφού για πρώτη φορά εφαρμόζεται η τεχνολογία των βάσεων δεδομένων (databases), αρχικά από μεγάλες εταιρείες, στη συνέχεια και από άλλους φορείς και οργανισμούς. Το διαδίκτυο, με τη βοήθεια των μηχανών αναζήτησης, αποκτά εμπορικό χαρακτήρα και σταδιακά καταλήγει στο σημερινό γνωστό ηλεκτρονικό εμπόριο (e-commerce) και υιοθετείται η χρήση των διακομιστών (Web Servers), έτσι ώστε να επιτρέπεται η ανάκτηση δυναμικού περιεχομένου (Χρήση τεχνολογιών ASP, PHP, CFML κ.α.)

Στο συμβατικό δίκτυο, οι σύγχρονες πλέον μηχανές αναζήτησης, ανακτούν το περιεχόμενο τους ακολουθώντας τους υπερ-συνδέσμους (hyperlinks) που βρίσκονται σε προηγούμενες ιστοσελίδες, αγνοώντας τις φόρμες αναζήτησης και τις σελίδες οι οποίες προϋποθέτουν χρήση κωδικού πρόσβασης στο περιεχόμενό τους (Price & Sherman, 2001, σσ. 26-35).

Αντιθέτως, στο Deep Web οι πληροφορίες είναι αποθηκευμένες σε βάσεις δεδομένων και η ανάκτηση τους γίνεται με λέξεις κλειδιά (Zilman, 2019). Σύμφωνα με τον ιδρυτή του Cambia Research, Steve Lautenschlager, το περιεχόμενο του Deep Web, ανάλογα με την μορφή του, ανοίκει στις πιο κάτω κατηγορίες:

I. **Δυναμικό περιεχόμενο**: αφορά δυναμικές σελίδες οι οποίες επιστρέφονται στο χρήστη υπό τη μορφή απάντησης σε ένα ερώτημα (query) ή μπορούν να ανακτηθούν μόνο μέσω μιας online φόρμας
II. **Περιεχόμενο περιορισμένης πρόσβασης**: ιστοσελίδες οι οποίες απαιτούν εγγραφή (registration) ή εμποδίζουν εσκεμμένα τις μηχανές αναζήτησης να προσπελάσουν το περιεχόμενο τους (π.χ. OpenAthens)
III. **Κωδικοποιημένο περιεχόμενο (Scripted)**: σελίδες οι οποίες μπορούν να προσπελαστούν μέσω συνδέσμων (links) τα οποία παράγονται από κώδικα Javascript ή Flash και χρειάζονται ειδική μεταχείριση
IV. **Μη συνδεδεμένο περιεχόμενο (unlinked content):** σελίδες οι οποίες δεν είναι συνδεδεμένες μέσω links με άλλες σελίδες, κάτι που μπορεί να εμποδίσει τους crawlers των μηχανών αναζήτησης από πρόσβαση στο περιεχόμενο τους.

V. **Περιεχόμενο όχι τύπου κειμένου (non-text):** αρχεία πολυμέσων (multimedia), έγγραφα σε μορφή διαφορετική από το παραδοσιακό HTML format, π.χ. PDF ή DOC (Lautenschlager, 2016).

Κεφάλαιο 4
Dark Web: ορισμός και χαρακτηριστικά

Το Dark Web ή σκοτεινό δίκτυο, αποτελεί πλέον μια εκ των πιο σκοτεινών πλευρών του διαδικτύου. Η δημιουργία του τοποθετείται αρχές της δεκαετίας του '90 και επί της ουσίας αποτελεί απόγονο του MILNET. Ιδρυτές του θεωρούνται οι μυστικές υπηρεσίες των Η.Π.Α. που είχαν ως στόχο την προστασία των διαφόρων συνομιλιών της κυβέρνησης με τον ναυτικό στόλο των Η.Π.Α. κατά τη διάρκεια των ταξιδιών του σε όλη την υφήλιο (BBC, 2019).

Ο αρχικός στόχος του δικτύου Tor ήταν να παρέχει μια ευέλικτη υποδομή επικοινωνιών, η οποία είναι ανθεκτική στις υποκλοπές, δηλαδή τη μη εξουσιοδοτημένη παρακολούθηση σε πραγματικό χρόνο μιας ιδιωτικής επικοινωνίας (ανάγνωση του ίδιου του μηνύματος), και στην ανάλυση της κυκλοφορίας, δηλαδή αποτροπή της διαδικασία παρακολούθησης και εξέτασης των επικοινωνιών, προκειμένου να προσδιοριστεί ποιος μιλάει με ποιον, πόσο καιρό διαρκούν οι συνομιλίες, πόσο συχνά συμβαίνουν και ποιες συμπεριφορές και συμφέροντα θα μπορούσαν να υποστούν.

Σχεδιάστηκε δηλαδή κατά τέτοιο τρόπο έτσι ώστε να διαγράφει εντελώς την ταυτότητα του χρήστη στο διαδίκτυο, παρέχοντας του έτσι ανωνυμία και ασφάλεια για όσο χρόνο βρίσκεται ο χρήστης βρίσκεται σε αυτό (BBC, 2019).

Όμως, όπως συμβαίνει συνήθως, η ανακάλυψη της ύπαρξης του έγινε αντιληπτή από μεγάλο αριθμό εγκληματικών στοιχείων σε ολόκληρο τον κόσμο, με αποτέλεσμα μέσα σε πολύ σύντομο χρόνο να περάσει στα χέρια και να τελεί υπό τον έλεγχο μιας σειράς παράνομων χρηστών, οι οποίοι βρίσκονται διασκορπισμένοι σε όλα τα μέρη της γης (Finklea, 2017).

Σήμερα, το Dark Web αποτελεί ένα παράλληλο κόσμο, μέσα στον οποίο βασιλεύει η παρανομία. Η ανωνυμία που παρέχει, "προστατεύει" άτομα που προέρχονται από το

χώρο της ιταλικής μαφίας, της κινέζικης, της μαφίας των Η.Π.Α. και όχι μόνο (Finklea, 2017).

Δεδομένων των πιο πάνω, μπορεί εύκολα κανείς να καταλήξει στο εξής οξύμωρο συμπέρασμά: Η διωκτικές αρχές των Η.Π.Α. και όχι μόνο, καλούνται να εντοπίσουν εγκληματίες που χρησιμοποιούν ένα λογισμικό το οποίο φτιάχτηκε από την ίδια την κυβέρνηση για να κρύβει τα ίχνη και να διατηρεί την ανωνυμία της στον ψηφιακό κόσμο.

4.1 Περιγραφή

Παρόλο που η ύπαρξή του Dark Web χρονολογείται από την δεκαετία του '90, εντούτοις έγινε ιδιαίτερα γνωστό στο ευρύτερο κοινό το 2013, όταν σε μια καλά οργανωμένη επιχείρηση το F.B.I. κατόρθωσε να εντοπίσει και να κλείσει την αγορά "Silk Road". Ο όρος "Silk Road" είναι εμπνευσμένος από το ιστορικό δίκτυο εμπορικών δρομολογίων που ξεκίνησε κατά τη διάρκεια της δυναστείας των Χαν (206 π.Χ. - 220 μ.Χ.) και αναφέρεται σε μια διαδικτυακή σύγχρονη πλατφόρμα μαύρης αγοράς για πώλησης παράνομων ναρκωτικών και όχι μόνο (Norry, 2018).

Για τη λειτουργία του συνελήφθη η Ross Ulbricht, γνωστή και ως Dread Pirate Roberts, η οποία κατηγορήθηκε για διακίνηση ναρκωτικών, κατασκοπεία στο διαδίκτυο και ξέπλυμα βρόμικου χρήματος (Carrington, Hogg, Scott, & Sozzo, 2018, σσ. 245-250).

Η εν λόγω ιστοσελίδα διέθετε προς πώληση πέραν των 10,000 προϊόντων, εκ των οποίων το 70% ήταν ναρκωτικά. Υπήρχαν επίσης προς πώληση νομικές υπηρεσίες, είδη ένδυσης, κλεμμένα έργα τέχνης, βιβλία, τσιγάρα, κοσμήματα, παράνομο λογισμικό και οπλισμός. Εκτιμάται ότι στα τρία χρόνια λειτουργίας του Silk Road (2011-2013), ανταλλάχθηκαν περισσότερα από 9,5 εκατομμύρια Bitcoins, τα οποία αντιστοιχούν σε περίπου 1,2 δισεκατομμύρια δολάρια (USD) στα πλαίσια του κύκλου εργασιών του και πέραν των 80 εκατομμύρια δολάρια σε προμήθειες (Carrington, Hogg, Scott, & Sozzo, 2018, σ. 247).

Σύμφωνα με τον αναλυτή συστημάτων ασφαλείας και μέλος της ομάδας Cyber G7 της ENISA (European Union Agency for Network and Information Security), Pierluigi Paganini, οι παράνομες συναλλαγές που διεξάγονται στο Dark Web, ξεπερνούν τα $100,000,000 το έτος. Μόνο από το Silk Road 1 και 2, υπολογίζεται ότι διεκπεραιώθηκαν πέραν των 1.5 εκατομμύρια συναλλαγές, το ύψος των οποίων ξεπερνά τα $1.2

δισεκατομμύρια. Υπολογίζεται δε ότι, τα τελευταία χρόνια, έχουν παραβιαστεί τα προσωπικά δεδομένα πέραν των 10 εκατομμυρίων ανθρώπων, κυρίως δελτία ταυτότητας και πιστωτικές κάρτες. Η μέση τιμή πώλησης μίας κάρτας στο Dark Web τιμάται στα $100 (Paganini, 2016).

4.2 Τρόπος λειτουργίας και χαρακτηριστικά

Σε αντίθεση με το συμβατικό δίκτυο και το Deep Web, το Dark Web λειτουργεί με ένα εντελώς διαφορετικό τρόπο, αξιοποιώντας όμως τις ίδιες διαδικασίες και υποδομές του παραδοσιακού διαδικτύου. Οι ιστοσελίδες οι οποίες φιλοξενούν υπηρεσίες Dark Web δεν έχουν τη μορφή διευθύνσεων όπως είναι τα γνωστά και φιλικά προς τον χρήστη URL, αλλά αποτελούνται από μια σειρά τυχαίων φαινομενικά χαρακτήρων, οι οποίες όμως είναι πλήρως κατανοητές και αναγνωρίσιμες από τα διάφορα εξειδικευμένα λογισμικά, όπως για παράδειγμα το TOR (Finklea, 2017).

Η επίσκεψη σε μια τέτοια σελίδα, επιτυγχάνεται διαμέσου μιας τυχαίας πορείας από διάφορους υπολογιστές ανά το παγκόσμιο, κατορθώνοντας έτσι να εξαφανίσουν τα ψηφιακά ίχνη του επισκέπτη. Βέβαια, στις πλείστες των περιπτώσεων, οι χρήστες συνδέονται εκ των προτέρων με εικονικά ιδιωτικά δίκτυα ή αλλιώς Virtual Private Networks (VPN). Αυτά, σε πρώτη φάση, τους επιτρέπουν να κρύψουν την ταυτότητα τους από τον παροχέα υπηρεσιών διαδικτύου τους (Internet Provider) και στη συνέχεια χρησιμοποιώντας κάποιο από τα εξειδικευμένα λογισμικά, όπως το TOR, προχωρούν στην τέλεση της όποιας παράνομης πράξης επιθυμούν. Ο συνδυασμός των δύο, VPN και TOR, καθιστά τον εντοπισμό του δράστη σχεδόν αδύνατο, γι' αυτό και το Dark Web εξακολουθεί να είναι ανεξέλεγκτο (Gehl, 2018, σσ. 7-14).

Σε μια προσπάθεια της να χαρτογραφήσει και να απεικονίσει το μερίδιο που αναλογεί στο κάθε ένα δίκτυο ξεχωριστά, η ιστοσελίδα techdracula.com, ετοίμασε το πιο κάτω γράφημα, σύμφωνα με το οποίο εκτιμά ότι, αναλογεί 5% στο συμβατικό δίκτυο, 94.97% στο Deep Web και μόλις 0.03% στο Dark Web.

Επίσης, διάφορα πανεπιστήμια, ιδιωτικοί οργανισμοί και εταιρείες υπηρεσιών ασφαλείας έχουν κατά διαστήματα επιχειρήσει να υπολογίσουν το μέγεθος των πληροφοριών που είναι κρυμμένες στο Dark Web. Περιορίζονται όμως, να καταπιαστούν και να καταγράψουν μία μεμονωμένη πτυχή ή παράμετρο του, με αποτέλεσμα πολλές

φορές οι αριθμοί να διαφέρουν από πηγή σε πηγή και αυτό είναι αναμενόμενο, αφού, λόγω του χαρακτήρα του Dark Web, κανείς δεν μπορεί να δώσει ένα ακριβές αριθμό. Παρόλα αυτά, οι Sui, Caverlee & Rudesill (2015) εκτιμούν ότι Dark Web κατά μέσο όρο ανέρχεται μόλις στο 0.01% του συνόλου του Deep Web.

4.3 Ανώνυμα δίκτυα και εφαρμογές πρόσβασης στο Dark Web

Όπως έχει προαναφερθεί, η πρόσβαση στο Dark Web επιτυγχάνεται με τη χρήση συγκεκριμένων λογισμικών, τα οποία είναι σχεδιασμένα να λειτουργούν κατά τέτοιο τρόπο έτσι ώστε να διαφυλάσσουν την ανωνυμία του χρήστη τους μέσα στα ανώνυμα δίκτυα. Αυτός ο τύπος ηλεκτρονικής ανωνυμίας διεκπεραιώνει την μεταφορά δεδομένων στο διαδίκτυο μέσω ενός παγκόσμιου δικτύου εθελοντών διακομιστών. Τα ανώνυμα δίκτυα εμποδίζουν την ανάλυση της κυκλοφορίας και την επιτήρηση του δικτύου ή τουλάχιστον τη δυσκολεύουν. Τα τρία βασικά ανώνυμα δίκτυα αναλύονται στη συνέχεια (Gamer, 2015).

4.3.1 The Onion Router (TOR)

Το Onion Router (TOR/Tor) είναι ένα δίκτυο ανοιχτού κώδικα που βασίζεται σε ένα πρωτόκολλο (σύνολο κανόνων) γνωστό ως "onion routing" και χρησιμοποιείται για ανώνυμη επικοινωνία μέσω ενός δικτύου υπολογιστών. Το Tor είναι το μεγαλύτερο και πιο διαδεδομένο αυτή τη στιγμή δίκτυο που χρησιμοποιείται στο Dark Web. Για να καταστεί δυνατή η πλοήγηση μέσα σε αυτό το δίκτυο, γίνεται χρήση της τεχνολογίας peer-to-peer (P2P), αξιοποιώντας τις δυνατότητες ενός συγκεκριμένου προγράμματος περιήγησης στο διαδίκτυο που ονομάζεται "Tor Browser" (Ciancaglini, Balduzzi, Goncharov, & McArdle, 2013).

Ο Tor Browser παρέχει τη δυνατότητα στο χρήστη να φιλοξενεί και ταυτόχρονα να περιάγει σε ανώνυμο ασφαλές περιβάλλον, παράνομο περιεχόμενο και υπηρεσίες, μέσα από ένα τεράστιο χώρο διευθύνσεων γνωστές ως "κρυφές υπηρεσίες". Τέτοιοι παράνομοι χώροι μπορεί να είναι ιστοσελίδες, ηλεκτρονικά φόρουμ και ηλεκτρονικές αγορές (eshops) (Ciancaglini, Balduzzi, Goncharov, & McArdle, 2013)..

Οι χρήστες του δικτύου Tor μπορούν να επισκεφθούν οποιοδήποτε κρυφό δικτυακό τόπο σε μια διεύθυνση *.onion. Αυτές οι διευθύνσεις δε μοιάζουν με συνήθεις διευθύνσεις URL, ούτε και μπορούν να προσπελαστούν με τους συμβατικούς περιηγητές διαδικτύου όπως το Edge, Internet Explorer, Google Chrome, Firefox, κ.λπ. Αποτελούνται από μια τυχαία εμφανιζόμενη σειρά 16 χαρακτήρων ακολουθούμενη από την επέκταση ".onion" και εκτελούνται μόνο μέσω του Tor Browser. Ένα παράδειγμα μιας κρυφής διεύθυνσης ιστότοπου είναι: http://dppmfxaacucguzpc.onion/ (Gamer, 2015).

4.3.2 Invisible Internet Project (I2P)

Το πρόγραμμα Invisible Internet Project (I2P) σχεδιάστηκε ως ανώνυμο στρώμα επικοινωνίας ομότιμης αλληλεπίδρασης (peer-to-peer-P2P) που μπορεί να εκτελέσει οποιαδήποτε παραδοσιακή υπηρεσία Internet. Έχει αναπτυχθεί από το 2003 και αποτελεί εξέλιξη του δικτύου Freenet, το οποίο έχει ως στόχο να επιτρέψει την εκτέλεση πολλών υπηρεσιών εκτός από το HTTP. Ενώ το TOR αρχικά σχεδιάστηκε για να επιτρέπει την ανωνυμία κατά τη σύνδεση με μια υπηρεσία Διαδικτύου (WWW) και μόνο αργότερα επεκτάθηκε στις γενικές κρυφές υπηρεσίες, ο αποκλειστικός στόχος του I2P είναι να παρέχει στους χρήστες τη δυνατότητα να φιλοξενούν υπηρεσίες (π.χ. IRC, Web, ταχυδρομείο , και bittorrent) με έναν κρυφό τρόπο (Ciancaglini, Balduzzi, Goncharov, & McArdle, 2013).

Το I2P παρέχει την δυνατότητα ανώνυμης περιήγησης στο διαδίκτυο, συνομιλίες, blogging και μεταφορά αρχείων. Το λογισμικό που υλοποιεί αυτό το επίπεδο επικοινωνίας ονομάζεται "δρομολογητής I2P (I2P router)" και ένας υπολογιστής που εκτελεί I2P καλείται "κόμβος I2P (I2P node)" (Gamer, 2015).

4.3.3 Freenet

Παρόμοια με το Tor και το I2P, υπάρχει από το 2000 ένα άλλο ανώνυμο δίκτυο που λέγεται Freenet. Είναι ένα από τα παλαιότερα δίκτυα και είναι γνωστό για τη δυνατότητα που παρέχει ανώνυμης ανταλλαγής αρχείων P2P, καθώς επίσης και για τη δημοσίευση "freesites" (ιστοσελίδες προσβάσιμες μόνο μέσω του Freenet) και chat σε φόρουμ (Gamer, 2015).

Σε σύγκριση με το I2P και το TOR, το Freenet προσφέρει λιγότερη ευελιξία όσον αφορά τις υπηρεσίες που φιλοξενούνται, περιορίζοντας την εξυπηρέτηση μόνο στατικού

περιεχομένου χωρίς, για παράδειγμα, scripting από πλευράς διακομιστή. Το φάσμα των υπηρεσιών που μπορούν να εφαρμοστούν σε αυτό είναι μικρότερο. Ωστόσο, αυτό δε σημαίνει ότι το Freenet δεν μπορεί να είναι μια κατάλληλη πλατφόρμα για να φιλοξενήσει απλές αγορές ή να ανταλλάξει πληροφορίες που σχετίζονται με κακόβουλες δραστηριότητες (Ciancaglini, Balduzzi, Goncharov, & McArdle, 2013)..

4.4 Κρυπτονομίσματα και η σχέση με το Dark Web

Με αφορμή την παγκόσμια οικονομική κρίση των τελευταίων 10-15 χρόνων, το 2008 γίνεται για πρώτη φορά επιστημονική δημοσίευση στην οποία περιγράφεται ο τρόπος λειτουργίας και χρήσης ενός εικονικού νομίσματος (Virtual Currency) ή κρυπτονομίσματος (Cryptocurrency) όπως επικράτησε να λέγεται. Ένα χρόνο μετά, κάνει την εμφάνιση του, για πρώτη φορά, ένα λογισμικό ανοικτού κώδικα που σκοπό είχε τη δημιουργία των αντίστοιχων ψηφιακών νομισμάτων ή αλλιώς Bitcoins. Ο συγγραφέας της δημοσίευσης, και δημιουργός του εν λόγω λογισμικού, παρέμεινε ανώνυμος, χρησιμοποιώντας το ψευδώνυμο Satoshi Nakamoto. Έτσι, γεννιέται το πρώτο ψηφιακό νόμισμα στην ιστορία της ανθρωπότητας και φέρει την ονομασία Bitcoin (Antonopoulos, 2015, σσ. 3-4).

Το κρυπτονόμισμα είναι στην ουσία ένα ψηφιακό νόμισμα το οποίο δεν υπάρχει επισήμως σε καμία φυσική μορφή, χαρτονομισμάτων ή κερμάτων, δεν παράγεται από καμία συγκεκριμένη χώρα, ούτε ελέγχεται από καμία συγκεκριμένη τράπεζα, κυβέρνηση ή οργανισμό. Η παραγωγή, αποθήκευσή και διακίνησή του, καθώς επίσης και όλες οι συναλλαγές με αυτό γίνονται αποκλειστικά και μόνο σε ηλεκτρονική μορφή. Χρησιμοποιείται πλέον όπως τα κανονικά παραδοσιακά νομίσματα, μπορεί κάποιος να το στέλνει μέσω e-mail σε ένα άλλο πρόσωπο, σχεδόν στιγμιαία, οποτεδήποτε και οπουδήποτε στον κόσμο. "Μεγάλωσε" με το Ίντερνετ και σήμερα αποτελεί την πιο διαδεδομένη μορφή χρήματος για το Ίντερνετ (Antonopoulos, 2015, σσ. 4-6).

Έκτοτε, λόγω και του ανοικτού κώδικα στον οποίο στηρίζει την ύπαρξη του, δημιουργήθηκε μια πληθώρα νέων κρυπτονομισμάτων στα οποία έχουν γίνει προσπάθειες για να βελτιωθούν ή/και να προστεθούν λειτουργίες όπως ταχύτερες συναλλαγές, μεγαλύτερη ανωνυμία κ.ά. Το κρυπτονόμισμα, σε γενικές γραμμές, είναι ένα εικονικό νομισματικό σύστημα, που τα κύρια χαρακτηριστικά του είναι: η σταθερότητα, η ασφάλεια και η ανωνυμία.

Στο Dark Web, οι οποιεσδήποτε συναλλαγές πραγματοποιούνται, προϋποθέτουν και την ανάλογη ανάγκη προστασίας όχι μόνο της πράξης ως γεγονός, αλλά και την προστασία των τεκμηρίων για την τέλεση τους. Ένας από τους βασικούς περιορισμούς ήταν η πληρωμή των αγορών που πραγματοποιούνται σε αυτό. Όπως ήταν αναμενόμενο, με την εμφάνιση των κρυπτονομισμάτων και ειδικά του Bitcoin, σιγά σιγά άρθηκαν οι οποίοι περιορισμοί και ανασφάλειες, και πλέον η συνύπαρξη και συνδυασμός των δύο είναι εκ των ουκ άνευ.

Το Bitcoin και τα υπόλοιπα κρυπτονομίσματα μεταμόρφωσαν το εμπόριο παράνομων αγαθών, ιδιαίτερα των ναρκωτικών. Χάρη σε αυτά και σε συνδυασμό με άλλα εργαλεία προστασίας της ανωνυμίας, π.χ. το TOR, έχουν καταστεί πλέον εφικτές εκατοντάδες χιλιάδες σκοτεινές και παράνομες αγορές στον κυβερνοχώρο και ιδιαίτερα το Dark Web (Stroukal & Nedvědová, 2016).

Διαχρονικά, μέσα από πολλές μελέτες και έρευνες που έχουν γίνει σχετικά με το θέμα, προκύπτει ότι η χρήση του Bitcoin, αλλά και άλλων κρυπτονομισμάτων από εγκληματίες για τις σκοτεινές αγορές τους στο διαδικτύο είναι ευρέως διαδεδομένη, ενώ στις πλείστες μάλιστα περιπτώσεις, αποτελεί και προϋπόθεση. Επιπρόσθετα, αρκετοί από αυτούς που επέλεξαν να κάνουν τις αγορές ή πωλήσεις τους στο Bitcoin, το έπραξαν με απώτερο σκοπό το ξέπλυμα βρώμικου χρήματος, αφού έτσι τους παρέχεται η δυνατότητα να ανταλλάσσουν και να κατακερματίζουν το αρχικό ποσό σε διάφορα άλλα κρυπτονομίσματα, καταφέρνοντας έτσι να εξαλείψουν τα ίχνη των συναλλαγών τους (Gomez, 2018).

4.5 Deep Web vs Dark Web

Πάρα πολύ συχνά παρατηρείται το φαινόμενο όπου παρομοιάζεται το Deep Web με το Dark Web. Αυτό είναι ένα τεράστιο λάθος, καθότι σε καμία περίπτωση δεν πρόκειται για το ίδιο πράγμα. Μπορεί μεν το δεύτερο να αποτελεί μέρος του πρώτου, όμως επί της ουσίας, απλά αξιοποιεί τις δυνατότητες και τα χαρακτηριστικά του.

Σύμφωνα με το διαδικτυακό λεξικό Dictionary.com, Deep Web ορίζεται το μέρος εκείνο του διαδικτύου το οποίο είναι κρυμμένο από τις συμβατικές μηχανές αναζήτησης και δεν καταχωρείται στο ευρετήριο ιστοσελίδων, είτε γιατί προστατεύεται από κωδικούς

πρόσβασης, είτε είναι καταχωρημένο σε βάσεις δεδομένων κ.λπ. Αντιθέτως, το Dark Web ορίζεται ως το μέρος εκείνο του διαδικτύου το οποίο σκόπιμα κρύβεται από τις μηχανές αναζήτησης και την κοινή πρόσβαση μέσω των γνωστών διευθύνσεων URL, αφού χρησιμοποιεί αποκρυμμένες διευθύνσεις IP και είναι προσβάσιμο μόνο με τη χρήση ειδικών προγραμμάτων περιήγησης στο διαδίκτυο, π.χ. TOR (Dictionary.com, 2019).

Αυτό που προκύπτει από τις πιο πάνω ερμηνείες, είναι ότι και τα δυο δίκτυα δεν είναι ανιχνεύσιμα από τις γνωστές μηχανές αναζήτησης, π.χ. Google, Bing, Yahoo, κ.λπ. Όσο αφορά τα υπόλοιπα χαρακτηριστικά, εκεί εστιάζονται και όλες οι διαφορές τους. Όπως αναφέρει ο Greenberg (2014) ο ερευνητής σε θέματα ασφάλειας Nik Cubrilovic, έχει καταμετρήσει λιγότερες από 10,000 κρυμμένες υπηρεσίες στο TOR, σε σύγκριση με τα εκατοντάδες εκατομμύρια των κανονικών ιστοσελίδων.

Καταληκτικά, το Deep Web αφορά υλικό προσβάσιμο μόνο κατόπιν εξουσιοδοτημένης ή περιορισμένης πρόσβασης και χρησιμοποιείται από άτομα όλων των κατηγοριών, ενώ το Dark Web αφορά διακίνηση παράνομου υλικού και συναλλαγών, και χρησιμοποιείται αποκλειστικά από παράνομους και εγκληματικά στοιχεία.

Κεφάλαιο 5
Dark Web: Παράνομες Δραστηριότητες

Μια από τις ιστοσελίδες με την πιο υψηλή επισκεψιμότητα στο Dark Web είναι το γνωστό WikiLeaks, το οποίο ιδρύθηκε το 2006 από τον Julian Assange και σκοπό έχει τη συλλογή απόρρητων ή/και εμπιστευτικών πληροφοριών από ανώνυμες πηγές και στη συνέχεια τη δημοσίευση τους στο ευρύτερο κοινό μέσω μιας δημόσιας ιστοσελίδας στο συμβατικό δίκτυο (WikiLeaks, 2015).

Στα έγκατα του Dark Web αποφάσισε να κινηθεί και μια άλλη, επίσης γνωστή και διαδεδομένη, ιστοσελίδα, αυτή του Facebook. Σύμφωνα με τον μηχανικό του, Alec Muffett, η δημιουργία της Facebook Tor έκδοσης της γνωστής πλατφόρμας κοινωνικής δικτύωσης, κρίθηκε επιβεβλημένη αφού η υφιστάμενη υποδομή δεν μπορούσε να λειτουργήσει αποτελεσματικά στον Tor, λόγω των αλγόριθμων που αφορούσαν την ασφάλεια των δεδομένων των χρηστών του. Ο σχεδιασμός της έγινε επίσης για να καλύψει τις ανάγκες πρόσβασης στην πλατφόρμα από χώρες όπως η Κίνα, Κορέα, Ινδία κ.λπ., οι οποίες απαγόρευσαν με νόμο τη χρήση της συγκεκριμένης πλατφόρμας (Greenberg, 2014).

5.1 Τομείς στους οποίους δραστηριοποιείται

Η εταιρεία ασφαλείας online συστημάτων, BatBlue, μέσα από μία μεγάλη πορεία παρακολούθησης και καταγραφής των περιστατικών κακόβουλης και κακοπροαίρετης χρήσης του παγκόσμιου ιστού, έχει κατατάξει τις παράνομες δραστηριότητες που διεξάγονται στο Dark Web σε τέσσερεις κύριες κατηγορίες, με βάση τη δραστηριότητα και την κατηγορία των ατόμων που ασχολούνται με αυτές. Σύμφωνα με τον Adarsh (2016), οι κατηγορίες αυτές είναι οι ακόλουθες.

5.1.1 Marketplace (Αγορά προϊόντων και υπηρεσιών)

Στην εν λόγω κατηγορία εμπίπτουν αδικήματα όπως:

- Drugs - Εμπορία Ναρκωτικών
- Money Laundering – Ξέπλυμα βρώμικου χρήματος
- Human Trafficking – Εμπορία προσώπων
- Malware/ Exploits – Κακόβουλο λογισμικό / εκμετάλλευση πολιτών
- Assassins / Hit Men – Πληρωμένους Δολοφόνους / εκτελεστές
- Weapons – Όπλα
- Illegal Activity How to – Οδηγίες για διεξαγωγή παράνομων δραστηριοτήτων
- Banned Pornography – Απαγορευμένη πορνογραφία,
- Child Pornography - Παιδική πορνογραφία
- Pirated Material – Πειρατικό υλικό, συνήθως λογισμικό Η/Υ

Συνήθως, ασχολούνται με αυτά, δημόσια πρόσωπα, κυβερνητικές υπηρεσίες και οργανισμοί, εγκληματίες, χάκερς και τρομοκράτες.

5.1.2 Cyber Warface (Κυβερνοέγκλημα - Κυβερνοτρομοκρατία)

Στην εν λόγω κατηγορία εμπίπτουν αδικήματα όπως:

- System Compromise – Παράνομη πρόσβαση σε συστήματα Η/Υ
- Information Disclosure – Διαρροή διαβαθμισμένων πληροφοριών
- Denial of Service – Παράνομη διακοπή λειτουργίας ενός συστήματος
- Delivery & Distribution – Παρεμβολή στην παράδοση – διάθεση προϊόντων
- Ransomware – Κακόβουλο λογισμικό που συνοδεύεται με απαίτηση λίτρων

Συνήθως, ασχολούνται με αυτά, κυβερνητικές υπηρεσίες και οργανισμοί, εγκληματίες και χάκερς.

5.1.3 Spying / Monitoring (Κατασκοπεία / Παρακολούθηση)

Στην εν λόγω κατηγορία εμπίπτουν αδικήματα που σχετίζονται με παρακολούθηση:

- Governments – Κυβερνήσεων
- Terrorists – Τρομοκρατών
- Corporate – Εταιριών
- Stalkers – Άτομα που παρενοχλούν ή καταπατούν τα δικαιώματα τρίτων

Συνήθως, ασχολούνται με αυτά, κυβερνητικές υπηρεσίες - οργανισμοί και τρομοκράτες.

5.1.4 Communications (Επικοινωνίες)

Στην εν λόγω κατηγορία εμπίπτουν αδικήματα που σχετίζονται με:

- Terrorists – Τρομοκράτες
- Political Dissent – Πολιτικούς αντιπάλους ή άτομα διαφορετικών πεποιθήσεων
- Adultery & Affairs – Εξωσυζυγικές σχέσεις και παράνομους δεσμούς
- Common Cause Collaboration – Συνεργασίες ατόμων με κοινούς σκοπούς
- Socially Disenfranchised – Κοινωνικός αποκλεισμός
- Bypass Censorship – Παράκαμψη της λογοκρισίας

Συνήθως, ασχολούνται με αυτά, δημόσια πρόσωπα, κυβερνητικές υπηρεσίες και οργανισμοί, χάκερς και τρομοκράτες.

5.2 Κίνδυνοι για τον απλό χρήστη

Η ιδιωτική ζωή των ανθρώπων είναι κάτι που απασχόλησε και θα εξακολουθήσει να κάνει και στο μέλλον όλη την ανθρωπότητα. Δεν είναι καθόλου τυχαίο που η ίδια η Ε.Ε. ασχολήθηκε με την νομική πτυχή του θέματος για σειρά ετών, όταν τελικά στις 14 Απριλίου 2016 το Ευρωπαϊκό Κοινοβούλιο υπερψήφισε τον ευρωπαϊκό γενικό κανονισμό προστασίας προσωπικών δεδομένων, το γνωστό GDPR. Ο κανονισμός τέθηκε σε εφαρμογή από τις 25 Μάϊου 2018 και προνοεί μια σειρά από αυστηρά μέτρα και ποινές για όσους τον παραβούν (EUGDPR, 2018).

Στόχος του GDPR είναι να προστατεύσει την ιδιωτική ζωή όλων των πολίτων της Ε.Ε. από τις παραβιάσεις των δεδομένων στο σημερινό ψηφιακό κόσμο, που το καθετί βασίζεται σε δεδομένα. Τι είναι σημαίνει όμως ο όρος προσωπικά δεδομένα; Σύμφωνα με τον GDPR, προσωπικό δεδομένο καλείται κάθε πληροφορία που χαρακτηρίζει έναν άνθρωπο, όπως για παράδειγμα, το ονοματεπώνυμο, η διεύθυνση, το τηλέφωνο, η θρησκεία, η ερωτική ζωή, οι πολιτικές πεποιθήσεις, οι ακαδημαϊκές επιδόσεις, τα ενδιαφέροντα, οι σχέσεις, οι δραστηριότητες, οι συναναστροφές, οι συνομιλίες, τα ιατρικά αρχεία, τα εισοδήματα και πολλά άλλα. Όλα αυτά καταγράφονται καθημερινά και τυγχάνουν επεξεργασίας, ανάλογα με το σκοπό και τους όρους για τους οποίους έχουν συλλεγεί (EUGDPR, 2018).

Η συλλογή τους γίνεται συνήθως με φόρμες/έντυπα στις οποίες οι ίδιοι οι άνθρωποι συναινούν να συμπληρώσουν για να εγγραφούν, όπως στα διάφορα κοινωνικά δίκτυα (Facebook, Twitter, Viber, κ.λπ.), σε online καταστήματα, σε online διαγωνισμούς και τυχερά παιχνίδια, σε αθλητικά σωματεία ή οργανωμένα σύνολα, σε ιατρικά αρχεία, στις υπεραγορές για έκδοση εκπτωτικής κάρτας και σε πολλά άλλα (EUGDPR, 2018).

Παρ' όλη τη δημοσιότητα, τις εγκυκλίους, τις προτροπές και τα σεμινάρια, τόσο των αρμοδίων υπηρεσιών του κράτους, όσο και άλλων ανεξάρτητων ιδιωτικών οργανισμών που ασχολούνται με την προστασία της ιδιωτικής ζωής, για τη μη ανάρτηση και δημοσίευση των προσωπικών δεδομένων από τους χρήστες, εντούτοις, δεκάδες χιλιάδες συμπολίτες μας σε όλες τις χώρες της Ε.Ε. έχουν πέσει θύματα. Συγκεκριμένα, στον πρώτο κιόλας χρόνο εφαρμογής του κανονισμού, έχουν καταγραφεί 144,376 καταγγελίες σε όλη την Ευρώπη (European Commision, 2019).

5.3 Τι μπορεί κάποιος να βρει στο Dark Web;

Το Dark Web είναι πλέον γνωστό για τη χρήση του σε εμπορικές συναλλαγές ναρκωτικών μεγάλης κλίμακας, για εμπόριο όπλων και φυσικά, για εμπορία ανθρώπων, οπότε εύκολα γίνεται αντιληπτό ότι εάν τολμήσει κάποιος να εισέλθει στα διαβολικά "νήματά" του, θα δει και κάποια φρικτά πράγματα. Αποτελεί τον ιδανικό χώρο, τόσο για όλους τους αδίστακτους που θέλουν να διαχειρίζονται παράνομες επιχειρήσεις ή να εκτελούν κακόβουλες υπηρεσίες όσο και για οποιονδήποτε μπορεί να ψάχνει, να χρειάζεται ή να ζητάει κάτι από αυτούς.

Μελέτες έχουν καταδείξει ότι δεν μπαίνουν όλοι στο Dark Web για κακοήθεις σκοπούς, αλλά κάποιοι, πιο αθώοι και καλόβουλοι, από τα εκατομμύρια που το χρησιμοποιούν, έχουν σκάψει βαθιά και έχουν τρομοκρατηθεί από τα πράγματα που είδαν εκεί μέσα. Για τον σκοπό αυτό, η γνωστή ιστοσελίδα AskReddit, θέλοντας να διερευνήσει και να ικανοποιήσει την περιέργεια των αναγνωστών της και όχι μόνο, είχε προβεί το 2015 στην εξής ανοικτή ερώτηση: "Χρήστες του Deep Web στο Reddit, ποιο είναι το πιο άρρωστο και τρομακτικό πράγμα που έχετε δει εκεί;" Τα αποτελέσματα και οι απαντήσεις που πήρε τρομακτικά (AskReddit, 2015).

Παραθέτονται ενδεικτικά μερικές από τις απαντήσεις που έχουν δοθεί:

- Υπάρχουν βουνά από ρωσικές ιστοσελίδες για σεξουαλική κακοποίηση παιδιών και πολλές ομάδες ανθρώπων ή μεμονωμένα άτομα που διαφημίζουν τις υπηρεσίες τους για να σκοτώσουν κάποιον ή να προστατεύσουν οποιονδήποτε.
- Τα πιο ενδιαφέροντα πράγματα που έχω βρει είναι ιστότοποι που ουσιαστικά σας βοηθούν να αλλάξετε εντελώς την ταυτότητά σας. Για παράδειγμα, για 6000 έως 10000 δολάρια μπορείτε να βγάλετε μια αμερικανική ταυτότητα, διαβατήριο, άδεια οδήγησης και όλα τα σχετικά έγγραφα, ώστε να μπορείτε να μετακομίσετε στην Αμερική με το όνομα που επιθυμείτε. Επίσης υπήρχε ένα ενδιαφέρον PDF αρχείο με πάνω από 1000 σελίδες που γράφτηκαν από πρώην κρατούμενους για το πώς να επιβιώσουν στη φυλακή, πώς να περνούν ναρκωτικά μέσα και έξω από φυλακές ή πώς να γίνουν μέλη σε συμμορίες μέσα στις φυλακές.
- Υπάρχουν κάποια top secret αρχεία για την επιχειρησιακή ασφάλεια, υπάρχουν μαθήματα κατασκευής εκρηκτικών, διαγράμματα για κάθε είδους συσκευή, οδηγίες για να κάνετε διάφορα εγκλήματα και όλων των ειδών τις απάτες και επίσης, όλα όσα αφορούν τις φυλακές ... Μέχρι τώρα είναι τόσο αηδιαστικό και τρομακτικό, που σίγουρα δεν θέλω να ξαναβρεθώ εκεί σύντομα.
- Έψαχνα για κάποιο διάστημα με τον TOR (The Onion Router) όταν οι ομοσπονδιακοί κυνηγούσαν για να κατεβάσουν τις πιο γνωστές ιστοσελίδες του σκοτεινού διαδικτύου. Κατάφερα να δω αναρχικά blogs. Απλά, ήταν γεμάτα από πολλές εικόνες βίας και τρομοκρατικής προπαγάνδας. Δεν με ενόχλησαν, όμως, οι τρομακτικές εικόνες, όσο η χαοτική και αναρχική αίσθηση σε όλο αυτό που συμβαίνει εκεί μέσα.
- Πιθανότατα το πιο άρρωστο πράγμα που έχω δει στο βαθύ Ιστό είναι μια διαφήμιση ιατρικών υπηρεσιών. Ισχυρίζονται ότι έχουν αρκετές αποθήκες γεμάτες από ανθρώπους, σε διαφορετικές χώρες και σε διαφορετικές συνθήκες (από άστεγους που είχαν απαχθεί στη Νέα Υόρκη μέχρι σκλάβους που αγοράστηκαν σε χώρες του τρίτου κόσμου). Για οποιοδήποτε χρηματικό ποσό, θα μπορούσατε να χρησιμοποιήσετε αυτούς τους ανθρώπους σε οποιοδήποτε ανήθικο ιατρικό πείραμα. Στη σελίδα τους έχουν επίσης κάποια έγγραφα σχετικά με δουλειές που έχουν κάνει. Είναι ένα από τα πιο ενοχλητικά πράγματα που βρήκα εκεί μέσα. Φαίνεται τόσο ρεαλιστικό γιατί ο σκοπός του δεν μοιάζει τόσο

κοινός για να είναι μια απάτη σαν τους πληρωμένους εκτελεστές (AskReddit, 2015).

Πιο κάτω επεξηγούνται μερικές από τις πιο διαδεδομένες και συνάμα αποτρόπαιες παράνομες δραστηριότητες που συντελούνται στα άδυτα του Dark Web.

5.3.1 Εμπόριο Ναρκωτικών

Όπως έχει προαναφερθεί, το εμπόριο ναρκωτικών μέσω της αγοράς Silk Road, αποτέλεσε σημείο σταθμό στην ιστορία του Dark Web, αφού το 2013 για πρώτη φορά είχε εντοπιστεί και καταστεί εφικτό το κλείσιμο μίας εκ των μεγαλύτερων αγορών παράνομων προϊόντων και ειδικά ναρκωτικών. Το Silk Road ήταν κάτι αντίστοιχο με το σημερινό Amazon ή το eBay, με τη διαφορά ότι αντί για βιβλία, ρούχα και ηλεκτρικά είδη, μπορούσε κάποιος να αγοράσει LSD, ecstasy ή όπλα κάθε λογής. (Carrington, Hogg, Scott, & Sozzo, 2018, σσ. 245-255).

Όπως χαρακτηριστικά αναφέρει σε άρθρο του ο Reid Southwick (2019), αρθρογράφος στην Καναδική εφημερίδα CBC News, υπάρχουν πλέον σαφείς και αυξανόμενες ενδείξεις ότι το εμπόριο ναρκωτικών κινείται όλο και περισσότερο στο Dark Web. Οι χρήστες σήμερα δε χρειάζεται να πάνε σε ένα στενό σοκάκι ή σε μια γωνιά του δρόμου και να συναντήσουν κάποιον που δεν έχουν ξαναδεί ποτέ πριν, κάτι που θα μπορούσε ενδεχομένως να τους βλάψει. Αντιθέτως, μπορούν να καθίσουν στον υπολογιστή τους ή ακόμη πιο εύκολα στο smartphone τους, και να αγοράσουν το ναρκωτικό της επιλογής τους και αυτό να παραδοθεί στο σπίτι τους.

Ενδεικτικό του μεγέθους και των οικονομικών συμφερόντων και απολαβών πίσω από τη λειτουργία τέτοιων ιστοσελίδων, αποτελεί το γεγονός ότι, παρόλο που τον Οκτώβριο του 2013 το FBI έκλεισε την ιστοσελίδα και συνέλαβε την Ross Ulbricht υπό την κατηγορία ότι ήταν η ιδρυτής της ιστοσελίδας με το ψευδώνυμο "Dread Pirate Roberts", ένα μήνα μετά, στις 6 Νοεμβρίου 2013, το Silk Road 2.0 τέθηκε εκ νέου σε λειτουργία στο διαδίκτυο. Μάλιστα, η λειτουργία του συνοδευόταν με ανάρτηση της μέσω του ψεύτικου λογαριασμού “Dread Pirate Roberts” στο Twitter (Μέσο κοινωνικής δικτύωσης), στην οποία έγραφε “20 minutes to go. You can never kill the idea of #silkroad.”. Ένα χρόνο μετά, στα πλαίσια συντονισμένης επιχείρησης με την ονομασία "Επιχείρησης Onymous",

αναστέλλεται εκ νέου η λειτουργία της παράνομης αυτής ιστοσελίδα και η φερόμενη επιχειρηματίας συλλαμβάνεται στις 6 Νοεμβρίου 2014 (Greenberg, 2014).

Μετά το κλείσιμο του Silk Road 2.0, μια άλλη ιστοσελίδα, η Diabolus Market μετονομάζεται σε "Silk Road 3 Reloaded" με σκοπό να εκμεταλλευτεί την επωνυμία και το πελατολόγιο του προηγούμενου. Στην συγκεκριμένη περίπτωση όμως, οι δημιουργοί της ιστοσελίδας, ενσωματώνουν μερικά νέα σχεδιαστικά και τεχνικά χαρακτηριστικά (συνδυάζουν τον Tor με το I2P), τα οποία υπόσχονται περισσότερη ασφάλεια (Cox, 2015)

Παράλληλα, τίθεται σε λειτουργία και μια άλλη παρόμοια ιστοσελίδα με την ονομασία AlphaBay. Τον Ιούλιο του 2017 ομοσπονδιακοί πράκτορες κατορθώνουν να τη θέσουν εκτός λειτουργίας και ακολουθούν συλλήψεις έως και 1,5 χρόνο μετά (Brandom, 2019).

5.3.2 Υπηρεσίες δολοφονίας

Ίσως μια από τις πιο ανησυχητικές υπηρεσίες στο Deep Web - και σίγουρα μια που δε θα μπορούσε με τίποτα να διαφημιστεί στο συμβατικό δίκτυο - είναι η "υπηρεσία" του πληρωμένου δολοφόνου. Υπάρχουν πολλές από αυτές τις υπηρεσίες στο Deep Web. Μάλιστα, όπως οι ίδιες οι ιστοσελίδες αναφέρουν, η φύση της "επιχείρησης" τους είναι τέτοια που προφανώς δεν μπορούν να δώσουν συστάσεις από προηγούμενους εργοδότες ούτε μπορούν να παρέχουν αποδείξεις της "ποιότητας" της δουλειάς τους. Αντ' αυτού, ζητούν από το άτομο να αποδείξει ότι έχει αρκετά Bitcoin διαθέσιμα για τη δουλειά, καταθέτοντας το συμφωνηθέν ποσό ως εγγύηση, αφού το Bitcoin αποτελεί μια αξιόπιστη υπηρεσία μεσεγγύησης, αφού μόνο όταν ο δράστης έχει πραγματοποιήσει τη δολοφονία και παράσχει αποδείξεις, τα χρήματα απελευθερώνονται (Balduzzi & Ciancaglini, 2015).

Σύμφωνα με τον υπεύθυνο ασφαλείας του περιοδικού Forbes, ένα από τα μεγαλύτερα δίκτυα "πρόσληψης" δολοφόνων ονομάζεται "Assassination Market". Σε αυτή την ιστοσελίδα, το όνομα του στόχου προστίθεται σε μια λίστα με ονόματα και στη συνέχεια, αφού "κατοχυρωθεί" η προσφορά και ανατεθεί το συμβόλαιο, οι χρήστες χρησιμοποιούν Bitcoins προκειμένου να χρηματοδοτήσουν τη δολοφονία. Ανάμεσα στα ονόματα της λίστας βρίσκονται αυτά του πρώην διευθυντή της NSA, Keith Alexander και του πρώην Αμερικανού προέδρου, Barack Obama, ενώ το όνομα του πρώην προέδρου της Federal Reserve, Ben Bernanke, έχει πλειοδοτηθεί με το ποσό των 75.000 δολαρίων (Greenberg, 2013).

Ο δημιουργός της σελίδας κυκλοφορεί με το ψευδώνυμο Kuwabatake Sanjuro και όπως ο ίδιος έχει αποκαλύψει μέσα από τα forums συζήτησης, φιλοδοξία του είναι η ανατροπή των κυβερνήσεων. Αφού ο Sanjuro βεβαιωθεί για τα αποτελέσματα της "δουλειάς" που ανατέθηκε στον υψηλότερο πλειοδότη, προβαίνει στην πληρωμή, αφού προηγουμένως κρατήσει προμήθεια 1% για κάθε δολοφονία (Greenberg, 2013).

Από έρευνες προκύπτει ότι κατά μέσο όρο, η αγορά υπηρεσιών δολοφόνου για τις περιπτώσεις που ο "στόχος" είναι ένας κοινός άνθρωπος ανέρχεται στις $20,000, ενώ όταν είναι κάποιος σπουδαίος ή διάσημο πρόσωπο, το ποσό ανεβαίνει στις $100,000 (Routley, 2017).

5.3.3 Παιδική πορνογραφία & πορνογραφία ενηλίκων

Σεβαστό χώρο στο Dark Web καταλαμβάνει και η παράνομη πορνογραφία. Εκεί μπορεί κανείς να βρει πορνογραφικό υλικό για κάθε λογής γούστο. Οι ιστοσελίδες του Dark Web και ειδικά αυτές της παιδικής πορνογραφίας είναι πολύ καλά οργανωμένες με πολλές δικλίδες ασφάλειας για τους παρόχους. Χρειάζεται να λάβεις πρόσκληση από κάποιον που είναι ήδη μέλος καθώς δεν αρκεί να πληκτρολογήσεις ένα όνομα χρήστη και έναν κωδικό πρόσβασης. Με άλλα λόγια αυτό σημαίνει πως πρέπει να πείσεις ότι έχεις και εσύ αντίστοιχες «άρρωστες» απόψεις και με κάποιον άλλο (Ormsby, 2018).

Σύμφωνα με έρευνα των Biryukov, Pustogarov, Thill, και Weinmann (2014), η διακίνηση πορνογραφίας μέσω του δικτύου το TOR, καταλαμβάνει την πρώτη θέση με ποσοστό 17% με δεύτερη την εμπορία ναρκωτικών με ποσοστό 15%. Ωστόσο, καταλήγουν στο συμπέρασμα ότι κανείς δεν μπορεί να επικαλεστεί με ασφάλεια το ακριβές ποσοστό, καθότι υπάρχουν τόσο τεχνικοί περιορισμοί, όσο και πρακτικοί, αφού είναι αδύνατον να καταγραφεί το πραγματικό μέγεθος.

Η αγορά υλικού παιδικής πορνογραφίας και εκμετάλλευσης είναι η πιο ανησυχητική πτυχή του Dark Web. Δεν είναι μόνο οι εικόνες και τα βίντεο που μεταφορτώνονται από τα χιλιάδες terabyte σε ένα αποκρουστικό οπτικοακουστικό θέαμα, αλλά και τα κοινωνικά φόρουμ όπου οι παιδόφιλοι μοιράζονται συμβουλές για το πως να κρατούν ήσυχα τα μικρά παιδιά, διατηρώντας τα ξύπνια, ψυχολογικά κόλπα για να τα ελέγχουν και τρόπους κάλυψης των εγκλημάτων τους. Αυτό όμως που ίσως προκαλεί το

μεγαλύτερο σοκ και αποτροπιασμό για την κατάντια του ανθρώπινου γένους, είναι να παρακολουθεί κανείς τα διάφορα Chat Rooms (ψηφιακές αίθουσες συνομιλίας) όπου οι παραβάτες περιγράφουν με παραστατικό και γραφικό τρόπο τις ερωτικές πράξεις τους με παιδιά, ειδικά όταν κάνουν χρήση λεξιλογίου που λογικά θα περίμενε να ακούσει κανείς να χρησιμοποιούνται από ενήλικα πρόσωπα σε ταινίες ερωτικού περιεχομένου ενηλίκων (Ormsby, 2018, σσ. 199-200).

5.3.4 Τρομοκρατία

Η χρήση της τεχνολογίας από τις διάφορες τρομοκρατικές οργανώσεις όπως οι ISIL και το ISIS, χρονολογείται από τα τέλη του 1990. Ωστόσο, η χρήση του συμβατικού δικτύου αποτελούσε εύκολο στόχο των διωκτικών αρχών και των μυστικών υπηρεσιών των διαφόρων χωρών με αποτέλεσμα συχνά οι τρομοκράτες να εντοπίζονταν και να συλλαμβάνονταν προτού εκπληρώσουν την αποστολή τους (Weimann, 2015).

Έτσι, μετά τις επιθέσεις του Νοεμβρίου του 2015 στο Παρίσι, η ISIS στράφηκε στο Dark Web για να διαδώσει ειδήσεις και προπαγάνδα σε μια προφανή προσπάθεια να προστατεύσει την ταυτότητα των υποστηρικτών της ομάδας και να διαφυλάξει το περιεχόμενό της. Στην ουσία, κάνουν εν μέρει ότι και πριν, αλλά πλέον στα κρυφά (Weimann, 2015).

Το Δεκέμβριο του 2015, μια ομάδα της Αλ Κάιντα που ονομάστηκε "ομάδα IT της Al-Aqsa" διέθεσε στο Dark Web ένα εγχειρίδιο με τίτλο "Tor Browser Security Guidelines", για την εξασφάλιση της OnLine ανωνυμίας κατά τη χρήση του λογισμικού TOR. Σε μια άλλη ανάρτηση τους, ανέβασαν αρχείο PDF με τίτλο "Bitcoin and the Charity of Violent Physical Struggle", το οποίο καθοδηγούσε τρόπους χρηματοδότησης της οργάνωσης μέσα από το Dark Web (Weimann, 2015).

Επιπρόσθετα, φαίνεται να έχουν αναπτύξει ένα τεράστιο σύστημα μέσα από το οποίο παρέχουν πληροφορίες σε "συναδέλφους" τρομοκράτες, προσλαμβάνουν και εκκολάπτουν ριζοσπάστες, στρατολογούν μαχητές, διαδίδουν προπαγάνδα, αντλούν κεφάλαια και συντονίζουν δράσεις και επιθέσεις (Brantly, 2017).

Τέλος, ένας από τους μεγαλύτερους εφιάλτες της αμερικανικής κυβέρνησης, είναι η περίπτωση χρήση drones για την διάδοση υψηλής περιεκτικότητας ραδιενεργού αερίου

πάνω από κατοικημένες περιοχές, η αγορά του οποίου προέρχεται μέσα από το Dark Web (Weimann, 2015).

Σύμφωνα με εκτιμήσεις, ο αριθμός των εξτραιμιστικών τρομοκρατικών ομάδων που δραστηριοποιούνται στο Dark Web, ανέρχεται στις 50,000 (Routley, 2017).

5.3.5 Ανθρώπινα πειράματα και κακοποίηση

Ένα άλλο είδος ιστοσελίδων που βρίσκει κανείς στο Dark Web, είναι αυτές που προωθούν οργανισμούς που πραγματοποιούν βασανιστικά πειράματα ή/και βασανιστήρια σε ζωντανούς ανθρώπους. Το πιο σοκαριστικό κομμάτι είναι οι ακριβείς περιγραφές των πειραμάτων. Είτε είναι αληθινά, είτε ψεύτικα, οι περιγραφές των πειραμάτων είναι ανατριχιαστικές, και οι εικόνες που τα συνοδεύουν ακόμη περισσότερο.

Η περίπτωση αυτή αποτελεί μια από τις πιο φρικιαστικές ίσως μορφές εγκλήματος στο Dark Web. Στο μυαλό του κάθε ανθρώπου που ακούει για πρώτη φορά για τα βασανιστήρια αυτά, ενστικτωδώς γεννιέται η απορία, κατά πόσο αυτό που διαβάσει ή ακούει είναι πραγματικό. Τουλάχιστο κανείς νοήμων άνθρωπος δεν θα μπορούσε να φανταστεί κάτι τέτοιο. Και όμως, σύμφωνα με αναρτήσεις στις εν λόγω ιστοσελίδες, φαίνεται να υπάρχουν ψυχοπαθείς, γιατί μόνο έτσι μπορούν να χαρακτηριστούν, που απολαμβάνουν να βλέπουν ανθρώπους να γίνονται πειραματόζωα και να σφαγιάζονται. Σύμφωνα με αναφορές, σε κάποιες ακραίες μάλιστα περιπτώσεις, αυτό γίνεται σε πραγματικό χρόνο, σε κάποια απομακρυσμένη γωνιά του κόσμου, με ζωντανή σύνδεση και online προβολή. Μάλιστα, παρέχεται η δυνατότητα στους "θεατές" όχι μόνο να παρακολουθήσουν την απάνθρωπη πράξη, αλλά να λάβουν μέρος και να προτείνουν μεθόδους βασανιστηρίων (DeepWebLinks, 2019).

Πιθανότατα αυτές οι ακραίες αναφορές να είναι υπερβολικές, αλλά η ύπαρξη παρόμοιων περιστατικών δεν μπορεί να απορριφθεί εντελώς και ο λόγος είναι απλός: υπάρχει το κίνητρο (οικονομική ή ψυχική ευτυχία), υπάρχει η ζήτηση (σαδιστές θεατές) και υπάρχουν και τα μέσα για να το καταστεί αυτό δυνατό (TOR ή άλλες τεχνολογικές εξελίξεις) (DeepWebLinks, 2019).

5.3.6 Εμπόριο ανθρώπων και ανθρώπινων οργάνων

Η εμπορία προσώπων, είναι ένα αδίκημα το οποίο χρονολογείται από τις αρχές του 19ου αιώνα και ήταν γνωστό ως εμπορία λευκής σαρκός. Βέβαια πολλά έχουν αλλάξει έκτοτε. Πλέον η εμπορία ανθρώπων περιλαμβάνει και τα δυο φύλα, ανεξαρτήτως ηλικίας, ακόμη και βρεφών. Επίσης, διαφοροποιείται και ο σκοπός για τον οποίο εμπορεύονται. Πέραν του αγοραίου έρωτα, άνθρωποι εμπορεύονται για καταναγκαστική εργασία, υπό το καθεστώς δουλείας, αλλά και για να ικανοποιούν τις σεξουαλικές ορέξεις της "εκλεκτής" πελατείας αυτών των παράνομων κυκλωμάτων. Σύμφωνα με στατιστικές των Η.Π.Α., κάθε χρόνο εμπορεύονται 600,000-800,000 άνθρωποι, μεταξύ των οποίων το 70% είναι γυναίκες και το 50% είναι παιδιά. Ένα μεγάλο μέρος αυτής της διακίνησης, οργανώνεται και συντονίζεται μέσα από το Dark Web (Carrington, Hogg, Scott, & Sozzo, 2018, σσ. 349-360).

Σε αυτή την κατηγορία, εμπίπτει και μια άλλης μορφής εμπορίας, αυτή της εμπορίας ανθρώπινων οργάνων, αφού οι μέθοδοι εντοπισμού των θυμάτων και οι χώρες προέλευσης είναι στις πλείστες των περιπτώσεων κοινές. Φαίνεται ότι μέσα στο Dark Web πραγματοποιούνται συμφωνίες και εμπορεύονται ανθρώπινα όργανα έναντι τεράστιων χρηματικών ποσών (Territo & Matteson, 2011, σσ. 32-35).

Και βέβαια, δεν εννοείται η περίπτωση οργάνων από άτομα που αποθνήσκουν, εννοείται ο οργανωμένος εντοπισμός συμβατού δότη ανάμεσα σε άτομα που προέρχονται συνήθως από φτωχές χώρες, στα οποία υπόσχονται ευκαιρία μετανάστευσης με υψηλές απολαβές και όταν αυτά εγκαταλείψουν τη χώρα τους, τα σκοτώνουν για να πάρουν το επιθυμητό όργανο που "παραγγέλθηκε" και στη συνέχεια το πωλούν στον ενδιαφερόμενο αγοραστή έναντι ποσού που ξεπερνά σε κάποιες περιπτώσεις και τις $200,000 (Territo & Matteson, 2011, σσ. 32-35).

Σε πρόσφατη έρευνα της παγκόσμιας οργάνωσης "STOP THE TRAFFIK" για το trafficking στο Dark Web, προκύπτει ότι το 93% των σχολιασμών έγιναν ανώνυμα, χωρίς δηλαδή καν ψευδώνυμο, 36% των αναρτήσεων περιλάμβαναν σεξουαλική εκμετάλλευση ανηλίκων, 44% αφορούσαν αποκλειστικά ιδιωτική "αγορά ή ενοικίαση" παιδιού και 4% αφορούσαν πώληση οργάνων (STOP THE TRAFFIK, 2018).

5.3.7 Αγορά πλαστών εγγράφων

Πλαστά διαβατήρια, άδειες οδήγησης, έγγραφα υπηκοότητας, δελτία ταυτότητας, πτυχία κολλεγίων, έγγραφα μετανάστευσης, μέχρι και οι διπλωματικές ταυτότητες, είναι μερικά από τα παράνομα έγγραφα που διατίθενται προς πώληση στις παράνομες ιστοσελίδες μέσα στο Dark Web. Ενδεικτικά, μια άδεια οδήγησης των Η.Π.Α., κοστίζει περίπου $200, ενώ τα διαβατήρια από τις Η.Π.Α. ή το Ηνωμένο Βασίλειο πωλούνται για μερικές χιλιάδες δολάρια (Jewkes & Yar, 2010, σσ. 288-293) .

Σύμφωνα με τους Jewkes και Yar, (2010), οι προσπάθειες για τον ποσοτικό προσδιορισμό του συνολικού κόστους του συγκεκριμένου εγκλήματος, αντιμετώπισαν μια σειρά προκλήσεων, καθώς τα επίσημα στατιστικά στοιχεία σχετικά με το έγκλημα σπάνια περιλαμβάνουν μια διακριτή κατηγορία εγκλημάτων ταυτότητας ή απάτης ταυτότητας, ενώ οι έρευνες συχνά ήταν μικρού μεγέθους και στερούνται εξειδίκευσης για να επιτρέπουν ακριβή υπολογισμό του κόστους αυτών των εγκλημάτων. Παρ' όλα αυτά, οι διάφορες εκτιμήσεις καταδεικνύουν ξεκάθαρα ότι υπάρχει ένας μεγάλος αριθμός θυμάτων κάθε χρόνο, συνήθως στις αναπτυγμένες χώρες, με απώλειες που υπερβαίνουν το $1 δισ. ετησίως ανά χώρα. Ένα μεγάλο μέρος του εγκλήματος εξακολουθεί να διαπράττεται εκτός του Dark Web και ο αριθμός των αδικημάτων και του κόστους αρχίζει να μειώνεται σε ορισμένες χώρες, πιθανώς λόγω των αυξημένων μέτρων ασφάλειας των υπολογιστών που χρησιμοποιούνται και της συνεχώς αυξανόμενης ευαισθητοποίησης των υπηρεσιών προστασίας των καταναλωτών (Jewkes & Yar, 2010, σσ. 288-293).

Παρόλα αυτά, το Διαδίκτυο εξακολουθεί να αποτελεί μια εκτεταμένη πηγή προσωπικών πληροφοριών και δεδομένων που είναι ικανές να καταχραστούν από εγκληματίες που επιδιώκουν να διαπράξουν εγκλήματα με οικονομικά κίνητρα (Jewkes & Yar, 2010, σσ. 288-293).

5.3.8 Χάκερς και Κράκερς

Πάρα πολύ συχνά, σε διάφορες συζητήσεις γύρω από θέματα τεχνολογίας, ακούμε ανθρώπους να αποκαλούν άτομα που ασχολούνται και έχουν αυξημένο επίπεδο γνώσης σε θέματα Η/Υ ως Χάκερ (Hacker). Αυτό συμβαίνει γιατί ανάμεσα στο ευρύ κοινό επικρατεί η λανθασμένη άποψη ότι "χάκερς" είναι αυτοί που εκμεταλλευόμενοι τις γνώσεις τους, προβαίνουν σε κακόβουλες πράξεις μέσω του διαδικτύου. Στην

πραγματικότητα, υπάρχουν δύο διαφορετικές κατηγορίες ανθρώπων που ασχολούνται με το θέμα, οι χάκερς και οι κράκερς. Συγκεκριμένα, χάκερ (Hacker) ονομάζεται συνήθως το άτομο το οποίο εισβάλει σε υπολογιστικά συστήματα και πειραματίζεται με κάθε πτυχή τους. Ωστόσο παλαιότερα είχε την έννοια του εφευρέτη, αυτού που ασχολείται έτσι ώστε να ανακαλύψει το πως λειτουργεί ένα σύστημα και να το βελτιώσει ή να το αλλάξει τροποποιώντας το (Code, 2002).

Αντιθέτως, οι "κράκερς" (Crackers), είναι άτομα τα οποία διεισδύουν ή διαφορετικά παραβιάζουν την ακεραιότητα ενός συστήματος απομακρυσμένων μηχανημάτων, με κακή πρόθεση. Έχοντας αποκτήσει παράνομη πρόσβαση, οι "κράκερς" καταστρέφουν σημαντικά δεδομένα, αποτρέπουν την εξυπηρέτηση των νόμιμων χρηστών ή προξενούν σοβαρά προβλήματα στα θύματά τους. Γενικά, η δράση των "κράκερς", συνοδεύεται από κακόβουλες πράξεις (Code, 2002).

Ωστόσο, οι χάκερς, έχουν τις κατάλληλες γνώσεις και ικανότητες να διαχειρίζονται σε μεγάλο βαθμό υπολογιστικά συστήματα. Συνήθως οι χάκερς είναι προγραμματιστές, σχεδιαστές συστημάτων αλλά και άτομα τα οποία ενώ δεν ασχολούνται επαγγελματικά με τομείς της πληροφορικής, έχουν αναπτύξει τέτοιες δεξιότητες και δουλεύουν είτε σε ομάδες (hacking-groups) είτε μόνοι τους. Αν οι πράξεις τους αυτές είναι κακόβουλες, αποκαλούνται κράκερ (Crawley, 2016) .

Στην σύγχρονη και ανταγωνιστική εποχή που ζούμε, μεγάλες εταιρείες προβαίνουν σε αγορά "υπηρεσιών" από τέτοια χαρισματικά άτομα με απώτερο σκοπό να προστατεύσουν και να διασφαλίσουν τα ηλεκτρονικά συστήματα τους, έναντι μεγάλης αμοιβής (Crawley, 2016).

Όπως ήταν αναμενόμενο, οι αγορά τέτοιου είδους υπηρεσιών, προσέκλισε και εγκληματικά στοιχεία τα οποία αξιοποιούν πλήρως την ανωνυμία του Dark Web και αναθέτουν σε φιλόδοξους χάκερς την εκτέλεση ποικίλων ηλεκτρονικών εγκλημάτων, όπως κυβερνοεπιθέσεις, εκβιασμοί, ακόμη και απόκρυψη από τις διωκτικές αρχές παράνομων κυκλωμάτων παιδεραστίας και γενικά οποιασδήποτε άλλης παράνομης δραστηριότητας διενεργείται μέσω του διαδικτύου (Crawley, 2016).

Το Dark Web σήμερα αποτελεί σίγουρα τον επίγειο παράδεισο των χάκερς, αφού μέσα από αυτό μπορούν ελεύθερα, χωρίς ωράριο και περιορισμούς να αναπτύξουν τις δεξιότητες τους έναντι αδρής πληρωμής και όλα αυτά από την άνεση του καναπέ τους (Code, 2002).

5.3.9 Botnet και ηλεκτρονικό "ψάρεμα"

Ο όρος Botnet, αναφέρεται σε ένα σύνολο από Η/Υ, των οποίων η ασφάλεια έχει παραβιαστεί και ελέγχονται πλέον εξ' αποστάσεως από τους hackers. Τα botnets αποτελούν μία από τις τελευταίες εξελίξεις στον Κυβερνοχώρο όσο αφορά τις εγκληματικές δραστηριότητες, καθώς, οι επίδοξοι δημιουργοί του κάθε botnet, αφού αρχικά "μολύνουν" τα ανυποψίαστα θύματα τους με κακόβουλο λογισμικό, στη συνέχεια τα θέτουν υπό τον πλήρη έλεγχο τους και στοχευμένα πλέον επιτίθονται μέσω αυτών στον κυρίως στόχο στον οποίο θέλουν να επιφέρουν και τη μεγαλύτερη ζημιά. Επί της ουσίας, δημιουργούν σιγά σιγά ένα μυστικό στρατό από πράκτορες ανά το παγκόσμιο και όταν έρθει η ώρα, ο δημιουργός του δίνει την ανάλογη οδηγία (Barford & Yegneswaran, 2007).

Αρχικά, η δράση τους περιοριζόταν συνήθως για φάρσες ή διάδοση μηνυμάτων για διαφημιστικούς σκοπούς. Αντιλαμβανόμενοι όμως τις τεράστιες δυνατότητες που τους παρείχε η χρήση της συγκεκριμένης μεθοδολογίας, πολύ γρήγορα αυτή επεκτάθηκε σε άλλο επίπεδο. Πλέον επιθέσεις botnet γίνονται επί πληρωμή έχοντας ως στόχο, να επιφέρουν ζημιά σε ανταγωνιστικές εταιρείες, κυβερνήσεις, πολιτικά πρόσωπα, θρησκευτικές ομάδες και γενικά οποιοδήποτε φυσικό ή νομικό πρόσωπο θεωρηθεί στόχος από τον πλειοδότη της επίθεσης. Το Dark Web, αποτελεί πεδίο λαμπρό στους επίδοξους δημιουργούς των botnet, αφού εκεί βρίσκουν άμεσα και ανώνυμα, άτομα που είναι διατεθειμένα να πληρώσουν αδρά τις "υπηρεσίες" τους (Hsinchun, 2012, pp. 427-439).

Σύμφωνα με τον Chen Hsinchun (2012), οι πιο διαδεδομένες μορφές επιθέσεων τύπου botnet είναι οι ακόλουθες:

- **Distributed Denial of Service (DDoS) attack –** αφορά κατανεμημένη επίθεση πολλαπλών αιτημάτων προς συγκεκριμένο στόχο με σκοπό να καταστήσουν ανενεργή την απρόσκοπτη παροχή υπηρεσιών δικτύου, ρυθμίζοντας χιλιάδες μολυσμένους Η/Υ να επιτίθονται ταυτόχρονα σε διακομιστές με αμέτρητα

άχρηστα αιτήματα για πληροφορίες. Τέτοια περίπτωση είχαμε και στην Κύπρο, όπου ανήλικος για λογαριασμό ξένης εταιρείας, πραγματοποίησε μια τέτοια επίθεση στο δίκτυο της εταιρείας παροχής υπηρεσιών διαδικτύου Cablenet, επιφέροντας της τεράστιές ζημιές, δυσφήμιση και προπαντός, ταλαιπωρία των πελατών της.

- **Infection** – αφορά μία μορφή "λοίμωξης". Όπως συμβαίνει και στο ανθρώπινο σώμα, έτσι και στο διαδίκτυο, τα συγκεκριμένα bots έχουν ως στόχο να ανιχνεύσουν ένα δίκτυο Η/Υ και να μολύνουν όλους τους ευάλωτους κατά τέτοιο τρόπο ώστε σιγά σιγά αυτοί να αφομοιώσουν το κακόβουλο λογισμικό καθιστώντας τους ικανούς να το χειραγωγήσουν. Τέτοιες επιθέσεις μπορούν να αξιοποιήσουν τη δημοτικότητα μιας συγκεκριμένης δημοφιλούς ιστοσελίδας, π.χ. μιας online εφημερίδας ή ενός portal, για να αξιοποιήσουν όσο το δυνατό περισσότερους επισκέπτες των σελίδων αυτών.
- **Spamming** – Τα botnets αποτελούν την πιο σημαντική πηγή υποκλοπής ηλεκτρονικών διευθύνσεων για αποστολή ανεπιθύμητων ή παράνομων μηνυμάτων email. Τέτοιου είδους μηνύματα μπορεί να περιλαμβάνουν phishing attacks (επιθέσεις "ψαρέματος" ευαίσθητων πληροφοριών ή/και λογαριασμών πρόσβασης) ή εγκατάσταση λογισμικού τύπου Trojan (Δούρειου ίππου). Αυτή η μορφή botnet χρησιμοποιείται συνήθως για διαφημιστικούς σκοπούς ή από χρηματιστηριακές εταιρείες οι οποίες θέλοντας να ελέγξουν τις τιμές στο χρηματιστήριο, διαδίδουν μέσω spam μηνυμάτων "ανάλογη" παραπληροφόρηση με σκοπό τον επηρεασμό των επενδυτών.
- **Espionage or Spyware** – αφορά ίσως την πιο επικίνδυνη μορφή botnet, καθώς αυτά παραμένουν σε ενέργεια για μεγάλο χρονικό διάστημα και δύσκολα γίνονται αντιληπτά από το θύμα. Στόχος τους είναι αφού εγκατασταθούν στα θύματα τους, να προβαίνουν σε αναζητήσεις εντός του Η/Υ ή του δικτύου στο οποίο βρίσκονται για διάφορα αρχεία και αποστολή τους στους εγκληματίες με σκοπό την ανάλογη αξιοποίηση τους. Επίσης, αποσκοπούν στην εξαγωγή όλων των αποθηκευμένων κωδικών πρόσβασης στο Internet από το προστατευμένο χώρο αποθήκευσης εντός του μολυσμένου Η/Υ και αποστολής τους στους εγκληματίες. Με απλά λόγια, πρόκειται για ένα κατάσκοπο εντός του Η/Υ, με απεριόριστες δυνάμεις. Σε πιο εξελιγμένη έκδοση τους, επιτυγχάνουν πρόσβαση σε κάμερες και ήχο από το περιβάλλον του θύματος με σκοπό την συλλογή υλικού που θα αποτελέσει προϊόν εκβιασμού και απαίτηση λύτρων.

5.3.10 Ransomware

Το Ransomware είναι ένας αρκετά διαδεδομένος τύπος κακόβουλου λογισμικού που έχει σχεδιαστεί για να αποκλείει την πρόσβαση σε ένα Η/Υ ή να κρυπτογραφήσει δεδομένα και αρχεία του θύματος έως ότου πληρωθούν τα "λύτρα". Η πληρωμή γίνεται συνήθως σε Bitcoin, χωρίς όμως να αποκλείονται και οποιαδήποτε άλλα κρυπτονομίσματα. Συνήθως, εξαπλώνεται μέσω μηνυμάτων ηλεκτρονικού "ψαρέματος" (phishing emails) ή όταν οι χρήστες επισκέπτονται εν αγνοία τους μια μολυσμένη ιστοσελίδα (Mohanta, Hahad, & Velmurugan, 2018).

Η πιο διαδεδομένη ίσως περίπτωση Ransomware, η οποία έχει μείνει γνωστή στην ιστορία για την ευρηματικότητα του δημιουργού της, είναι αυτή του "Reveton" ή αλλιώς "υιός της Αστυνομίας" (Police Ransomware). Στη συγκεκριμένη περίπτωση, το κακόβουλο λογισμικό, αφού κρυπτογραφούσε όλα τα αρχεία δεδομένων που βρίσκονταν στον Η/Υ του θύματος, εμφάνιζε ένα μήνυμα στην οθόνη του υπολογιστή με λογότυπα των αρχών επιβολής του νόμου στο οποίο ανάφερε ότι ο χρήστης του εν λόγω Η/Υ παραβίασε μία σειρά από εγχώριες και διεθνείς νομοθεσίες και ότι θα έπρεπε άμεσα να προβεί στην καταβολή συγκεκριμένου εξώδικου ποσού σε λογαριασμό Bitcoin, αφενός για να αποφύγει την καταδίκη, αφετέρου για να επανέλθει ο Η/Υ και τα αρχεία στην αρχική τους κατάσταση (Mohanta, Hahad, & Velmurugan, 2018).

Αυτό που κάνει ιδιαίτερη την περίπτωση αυτή, είναι το γεγονός ότι το κακόβουλο λογισμικό ήταν σε θέση αρχικά να αναγνωρίσει τη γεωγραφική θέση του θύματος και στη συνέχεια να προσαρμόζει τα λογότυπα και τις πληροφορίες που αφορούσαν την παραβίαση στην τοπική γλώσσα, καθιστώντας έτσι πειστική την προειδοποίηση για καταδίκη σε περίπτωση μη καταβολής του ποσού για την εξώδικη διευθέτηση του αδικήματος (Mohanta, Hahad, & Velmurugan, 2018).

Η περίπτωση αυτή απασχόλησε και την Κυπριακή Αστυνομία, αφού δεν είναι λίγα τα θύματα τα οποία είχαν άγνοια για την συγκεκριμένη απάτη και προέβηκαν στην καταβολή των λύτρων (Αστυνομία Κύπρου, 2013).

Κεφάλαιο 6
Τρόποι Αντιμετώπισης

Σε αντίθεση με το παραδοσιακό έγκλημα, η ανώνυμη φύση του Dark Web και τα εγγενή δικαιοδοτικά ζητήματα περιορίζουν σε μεγάλο βαθμό την ικανότητα των αρχών επιβολής του νόμου να εντοπίσουν την αιτία ή τον συσχετισμό ατόμων πίσω από μια παράνομη ιστοσελίδα. Η αστυνομία καθημερινά ασχολείται με μια ευρεία ποικιλία εγκλημάτων, όπως μικροκλοπές, τροχαίες παραβάσεις, διαρρήξεις, βιαιοπραγίες, φόνους, κ.λπ. Όμως, λόγω και του μεγάλου φόρτου εργασίας, συνήθως εστιάζεται στα άμεσα γεγονότα του εγκλήματος και στα τελικά αποτελέσματα. Για παράδειγμα, ένα κλεμμένο όπλο που ανακαλύφθηκε κατά τη διάρκεια μιας έρευνας σε οικία, αντιμετωπίζεται ως περίπτωση παράνομης κατοχής όπλου, ωστόσο το γεγονός ότι το όπλο αγοράστηκε και πωλήθηκε μέσω του Dark Web, δεν καταγράφεται στα στατιστικά στοιχεία. Κατά συνέπεια, ο εντοπισμός της πηγής και της προμήθειας του όπλου, θα πρέπει να θεωρείται και να αντιμετωπίζεται ως θέμα ζωτικής σημασίας, έτσι ώστε να επιτευχθεί η συνολική μείωση της εγκληματικότητας (Kehoe, 2018).

Η παγκοσμιοποίηση των χρηματοπιστωτικών αγορών έχει διευκολύνει την ανάπτυξη του διακρατικού εγκλήματος. Οι εγκληματικές οργανώσεις έχουν προσαρμόσει γρήγορα τις δομές και τις δραστηριότητές τους σε νέες ευκαιρίες στην παγκόσμια οικονομία. Το Dark Web παρέχει όλα τα εχέγγυα και την απαιτούμενη προστασία για να ασχοληθούν όλο και περισσότερο με διασυνοριακές δραστηριότητες, τόσο ως απάντηση στις παράνομες ευκαιρίες της αγοράς όσο και ως μέσο μείωσης της ευαισθησίας τους στα μέτρα αντιμετώπισης της επιβολής του νόμου. Ως αποτέλεσμα, οι εγκληματικές οργανώσεις και τα δίκτυα έχουν αυξηθεί σε μέγεθος και δύναμη και πολλοί έχουν αναπτύξει ενδιαφέροντα πέρα από τη χώρα καταγωγής τους (Wardlaw, 1999).

6.1 Διεθνής Συνεργασία

Παρόλο που η ύπαρξη και η δράστη του Dark Web αποτελεί ένα παγκόσμιο φαινόμενο, εντούτοις, δε γίνεται αντιληπτό από όλες τις χώρες το μέγεθος και ο βαθμός

επικινδυνότητας του προβλήματος. Βέβαια, για την αξιολόγηση του προβλήματος από την εκάστοτε χώρα, λαμβάνονται υπόψη και μια σειρά από πολλές άλλες παραμέτρους, που έχουν να κάνουν συνήθως με την κουλτούρα και τον πολιτισμό της κάθε μίας ξεχωριστά. Επίσης, σημαντικό ρόλο παίζουν τα γεωπολιτικά δεδομένα της κάθε χώρας και οι διακρατικές και διεθνείς σχέσεις που ανέπτυξε. Για παράδειγμα η περίπτωση της Κίνας, όπου πρόκειται για μία χώρα στην οποία η χρήση ηρωίνης είναι ευρέως διαδεδομένη και είναι απίθανο να επηρεαστεί από τις τρέχουσες ρυθμίσεις της κινεζικής πολιτικής και αναμένεται να συνεχίσει να αυξάνεται. Η κύρια προέλευση τους είναι η Βιρμανία, ωστόσο, υπάρχουν και διάφορες άλλες πηγές όπως το Αφγανιστάν, το Πακιστάν, το Καζακιστάν, το Τατζικιστάν και η Βόρεια Κορέα. Χώρες δηλαδή με τις οποίες η επικοινωνία και συνεργασία είναι σχεδόν ανύπαρκτή, με αποτέλεσμα η ροή και χρήση ηρωίνης συνεχίζει να αυξάνεται ραγδαία (Wardlaw, 1999).

Το 2013, η EUROPOL (Ευρωπαϊκή Αστυνομία), θέλοντας να βοηθήσει στην προστασία των ευρωπαίων πολιτών και να ενισχύσει την καταπολέμηση του ηλεκτρονικού εγκλήματος στα Κράτη Μέλη της, προχώρησε στη δημιουργία του Ευρωπαϊκού Κέντρου Καταπολέμησης του Κυβερνοεγκλήματος (EC3). Ένας από τους κύριους τομείς που δραστηριοποιείται, είναι και το Dark Web (EC3, 2019).

Επίσης, τα τελευταία χρόνια, διεθνής οργανισμοί όπως η EUROPOL (Ευρωπαϊκή Αστυνομία), η ASEANAPOL (Αστυνομική Οργάνωση των Εθνών της Νοτιοανατολικής Ασίας),η FATF (Ομάδα Χρηματοοικονομικής Δράσης των G7) και ο οργανισμός Ηνωμένων Εθνών μέσα από διάφορες διεθνείς συμβάσεις, έχουν ξεκινήσει μία μεγάλη δραστηριότητα και σειρά από κοινές δράσεις που στοχεύουν στην ανάπτυξη συνεργασιών για νομοθετική ρύθμιση και αντιμετώπιση του φαινομένου. Παρ' όλα αυτά, οι προσπάθειες τείνουν να είναι αργές και σχετικά δύσκολες (Wardlaw, 1999).

Προϊόν τέτοιας συνεργασίας, είναι και τα αποτελέσματα μιας συντονισμένης επιχείρησης που διεξάχθηκε τον Μάρτιο του 2019, κατά την οποία αρχές επιβολής του νόμου από την Ευρώπη, τον Καναδά και τις Ηνωμένες Πολιτείες ένωσαν τις δυνάμεις τους με στόχο τους πωλητές και τους αγοραστές παράνομων αγαθών στις σκοτεινές ιστοσελίδες. Κατά τη διάρκεια αυτής της επιχείρησης, οι διεθνείς υπηρεσίες επιβολής του νόμου προέβησαν σε 61 συλλήψεις και έκλεισαν 50 σκοτεινές ιστοσελίδες που χρησιμοποιήθηκαν για παράνομες δραστηριότητες. Η Αστυνομία εκτέλεσε 65 εντάλματα έρευνας,

κατασχέθηκαν 299,5 κιλά ναρκωτικών, 51 πυροβόλα όπλα και πάνω από 6,2 εκατομμύρια ευρώ (περίπου 4 εκατομμύρια ευρώ σε κρυπτονομίσματα, 2,2 εκατομμύρια ευρώ σε μετρητά και 35,000 σε χρυσό). Για τα πιο πάνω, λήφθηκαν συνολικά 122 καταθέσεις (Europol, 2019).

Ιδιαίτερα σημαντική θεωρείται και μια πρόσφατη, ανάλογη επιχείρηση, όπου, το Μάϊο του 2019, μετά από συντονισμένη παρακολούθηση δυο ολόκληρων χρόνων, απόδειξη του μεγάλου βαθμού δυσκολίας που έχει η χρήση του Dark Web, οι αρχές κατάφεραν να συλλάβουν 9 πρόσωπα σχετικά με αδικήματα που σχετίζονται με κακοποίηση, εμπορία και βιασμό ανηλίκων παιδιών. Οι δράστες προέρχονταν από Ταϊλάνδη, Αυστραλία και Ηνωμένες Πολιτείες. Το σημαντικότερο όμως αυτής της συντονισμένης επιχείρησης που διενεργήθηκε από την INTERPOL, είναι το γεγονός ότι έχει οδηγήσει στη διάσωση 50 παιδιών, θυμάτων αυτού του μινώταυρου που ονομάζεται παιδική πορνογραφία (Interpol, 2019).

6.2 Επαγγελματική κατάρτιση

Καθώς η ευαισθητοποίηση του κοινού μεγαλώνει και τα μέσα μαζικής ενημέρωσης θα προβάλουν όλο και περισσότερο τους κινδύνους που ελλοχεύουν από την ύπαρξη και χρήση αυτού του σκοτεινού ιστού, η ανάγκη για επαγγελματική κατάρτιση και ενημέρωση όλων των μελών των αρχών επιβολής του νόμου είναι επιβεβλημένη. Επιπρόσθετα, κάθε οργανισμός, ανεξαρτήτως μεγέθους, οφείλει να δημιουργήσει, αν δεν το έχει κάνει ήδη, μια ειδική μονάδα για τη διερεύνηση εγκλημάτων στο Διαδίκτυο. Η ομάδα αυτή θα πρέπει να στηρίζεται σε τρεις βασικούς πυλώνες, την εκπαίδευση, τη στελέχωση και την εμπειρογνωμοσύνη (Kehoe, 2018).

Οι αστυνομικοί πρέπει να μάθουν να αναγνωρίζουν και να αντιμετωπίζουν τα εγκλήματα στο Dark Web, γι' αυτό και η εξειδικευμένη εκπαίδευση τους είναι καίριας σημασίας από την άποψη αυτή. Ο σύγχρονος αστυνομικός, πρέπει να είναι σε θέση να κατανοεί τα βασικά χαρακτηριστικά στοιχεία του Dark Web και να αναγνωρίζει τους εγκληματίες ή τα εγκλήματα που μπορεί να έχουν σχέση με αυτό. Επιπρόσθετα, η βασική αυτή γνώση θα τους υποβοηθήσει και στην περίπτωση που θα καλέσουν κάποιο εμπειρογνώμονα, αφού θα είναι σε θέση να κατανοήσουν καλύτερα τα ευρήματα του και τη φύση του αδικήματος, καθιστώντας τους πιο αποτελεσματικούς στην πορεία των ανακρίσεων και εν τέλει, στην απόσπαση της μαρτυρίας. Τέτοιου επιπέδου εκπαίδευση, καλό θα ήταν να

περιλαμβάνεται στη βασική εκπαίδευση που προσφέρουν οι αστυνομικές ακαδημίες (Kehoe, 2018).

Περαιτέρω, οι ανακριτές που θα ειδικευτούν στη διερεύνηση του Dark Web, θα πρέπει να συμμετέχουν σε ομάδες εργασίας στο εξωτερικό, όπου μέσα από τις συχνές συναντήσεις θα ανταλλάζουν εμπειρογνωμοσύνη και θα παίρνουν ανατροφοδότηση των εξελίξεων γύρω από το φαινόμενο (Kehoe, 2018).

6.3 Χρήση προηγμένων τεχνολογιών

Ένας από τους πιο βασικούς παράγοντες που συμβάλουν στην άμεση και γρήγορη διερεύνηση τέτοιων υποθέσεων, είναι και η αξιοποίηση στο έπακρο της τεχνολογίας εκ μέρους των διωκτικών αρχών. Είναι αδιανόητο να περιμένει κανείς να αντιμετωπίσει ένα ολόκληρο σύγχρονο στρατό, με μια διμοιρία τυφεκιοφόρων. Είναι εκ των πραγμάτων αδύνατο. Άρα στην αποτελεσματικότητα των δικανικών ανακριτών συμβάλει τόσο η επαγγελματικής τους κατάρτιση, όσο και ο εκσυγχρονισμός του τεχνολογικού εξοπλισμού που έχουν στην διάθεση τους.

Κλασικό παράδειγμα αξιοποίησης της τεχνολογίας, αλλά και άλλων θετικών επιστημών, αποτελεί η περίπτωση μελέτης της Jihad. Η μεθοδολογία που αναπτύχθηκε ενσωμάτωσε τεχνικές συλλογής, ανάλυσης και οπτικοποίησης πληροφοριών, καθώς επίσης και εκμετάλλευση διαφόρων πηγών πληροφοριών από το Διαδίκτυο. Συγκεκριμένα, εφαρμόστηκε συλλογή και ανάλυση πληροφοριών από 39 διαφορετικές ιστοσελίδες της Jihad και αναπτύχθηκε απεικόνιση του περιεχομένου των ιστοσελίδων, των σχέσεων και των επιπέδων δραστηριότητάς τους. Η πιο πάνω μελέτη, πέραν των σημαντικών πληροφοριών που κατάφερε να αναδείξει, κατέδειξε ότι η μεθοδολογία είναι πολύ χρήσιμη και ελπιδοφόρα και έχει μεγάλες δυνατότητες να βοηθήσει στη διερεύνηση και κατανόηση των τρομοκρατικών δραστηριοτήτων. Επίσης, τα ευρήματα της ανάλυσης, θα μπορούσαν ενδεχομένως να βοηθήσουν στην καθοδήγηση τόσο της χάραξης πολιτικής όσο και της περαιτέρω διερεύνησης των πληροφοριών (Chen, et al., 2008).

Κεφάλαιο 7
Επίλογος

Λαμβάνοντας υπόψη κανείς τα πιο πάνω, διαπιστώνει ότι οι πραγματικότητες του Διαδικτύου παρουσιάζουν σαφή ένδειξη για το πόσο λίγη είναι η κατανόηση της νέας τάξης πραγμάτων στο διαδίκτυο. Πρόκειται για ένα εντελώς καινούργιο τρόπο ζωής όπου η αλματώδης αλληλεπίδραση κοινωνίας και τεχνολογίας δύσκολα γίνεται κατανοητή. Βλέπουμε από τη μια τους πολίτες να αποκτούν τεράστια και δυσανάλογα δικαιώματα για την άσκηση πρακτικών που στο παρελθόν θεωρούνταν παράνομες, και από την άλλη παρατηρούμε την αδιαφορία και την άρνηση τους να αντισταθούν σε αυτό, πιθανόν, από φόβο για το άγνωστο,

Παρόλο που η αξία των άυλων αγαθών, όπως τα ψηφιακά πνευματικά δικαιώματα ή το ηλεκτρονικό χρήμα, έχει αναγνωριστεί αρκετά γρήγορα, η αξία των πληροφοριών - ειδικά εκείνων που αφορούν την προσωπική μας ζωή - παραμένει ασαφής για τους περισσότερους από εμάς. Ο βαθμός εξάρτησης και η κατάχρηση της τεχνολογίας που παρατηρείται στη σημερινή εποχή, όπου όλοι είναι συνεχώς με ένα κινητό στο χέρι, είναι πιθανό να επιδεινώσουν την κατάσταση.

Σε έναν κόσμο όπου ακόμη και τα ρούχα που φοράμε μπορεί να περιέχουν ετικέτες εντοπισμού RFID, η προσωπική ζωή καθίσταται διάχυτη. Η επιτήρηση του Διαδικτύου μπορεί να είναι μόνο η άκρη ενός πολύ μεγάλου παγόβουνου, αλλά παρέχει μια ένδειξη της ασφάλειας ή των εμπορικών "επιταγών" που μέχρι στιγμής έχουν πετύχει την ισορροπία μεταξύ συμβατικού και σκοτεινού δικτύου.

Το Dark Web είναι από τη φύση του ανώνυμο και ανίκανο να διακρίνει τη διαφορά μεταξύ εγκληματία και απλού χρήστη. Οι αρχές επιβολής του νόμου πρέπει να αντιμετωπίσουν αυτό το ζήτημα συλλογικά, εφαρμόζοντας τακτικές που διατηρούν την ιδιωτικότητα του μέσου χρήστη ενώ ταυτόχρονα να αποκαλύπτουν τον εγκληματία.

Πρέπει να συντονίζουν τις προσπάθειες τους και να ενεργούν ταυτόχρονα, καθώς έτσι στέλνεται ένα ισχυρό μήνυμα σε όσους ασχολούνται με την πώληση και την αγορά ναρκωτικών, πλαστών προϊόντων, πυροβόλων όπλων κ.λπ. στο Dark Web. Ο πιο αποτελεσματικός τρόπος για να γίνει αυτό είναι η αναζήτηση των παράνομων ιστοσελίδων αντί των παράνομων χρηστών. Η οποιαδήποτε επιτυχία αναστολής της λειτουργίας τέτοιων ιστοσελίδων, σε συνδυασμό με τις αυστηρές ποινές, θα λειτουργήσει αποτρεπτικά για όλους τους υπόλοιπους (Chertoff, 2017).

Βέβαια, υπάρχει και η άποψη μερίδας ανθρώπων που εισηγούνται ως μέτρο καταστολή, την απαγόρευσης της χρήσης του Tor. Η εμπειρία όμως έχει καταδείξει ότι η τεχνολογία λειτουργεί όπως και η λερναία Ύδρα, για κάθε ένα κεφάλι που κόβεις, άλλα δύο το αντικαθιστούν. Επιπρόσθετα, θα καταστρέψει επίσης ένα χρήσιμο εργαλείο για τους νόμιμους χρήστες, οι οποίοι θέλουν να διατηρούν την ανωνυμία τους, ειδικά όταν πρόκειται για αντιφρονούντες ή άτομα θέλουν να προστατεύσουν την ανωνυμία τους ή την ιδιωτική τους ζωή.

Καταληκτικά, το Dark Web θα συνεχίσει να δελεάζει και να συναρπάζει όλους όσους χρησιμοποιούν το Διαδίκτυο, αφού περιέχει μια εντυπωσιακή ποσότητα γνώσεων που θα μπορούσε να μας βοηθήσει να εξελιχθούμε τόσο τεχνολογικά, όσο και κοινωνικά ως άνθρωποι, όταν αυτές συνδυάζονται και με άλλες επιστήμες. Φυσικά, η κρυφή διάσταση του θα παραμείνει, γιατί άλλωστε, αυτό είναι ένα από τα έμφυτα χαρακτηριστικά της ανθρώπινης μας φύσης.

Το Dark Web προβάλει την απύθμενη, διάσπαρτη δυνατότητα όχι μόνο του Διαδικτύου, αλλά και του ίδιου του ανθρώπινου γένους. Ανεξάρτητα από το αν θα υπάρχει ή όχι το Dark Web, όλες οι προαναφερθείσες παράνομες δραστηριότητες θα εξακολουθούν να εμφανίζονται και να υπάρχουν. Το Dark Web παρέχει απλώς έναν εύκολο τρόπο σύνδεσης με ανθρώπους παρόμοιων συμφερόντων και διευκολύνει την περαιτέρω αλληλεπίδραση τους. Η ορθή και υγιής χρήση του θα πρέπει να είναι αποτέλεσμα εσωτερικής πειθαρχίας, αλλά και κοινωνικών νορμών που θα αναπτυχθούν με την πάροδο του χρόνου, μέσα από την χάραξη μιας εθνικής, γιατί όχι και παγκόσμιας στρατηγικής.

Βιβλιογραφία

Adarsh, V. (2016, September 30). *Welcome to the Darknet: The Underground for the "Underground".* Ανάκτηση May 18, 2019, από Fossbytes: https://fossbytes.com/welcome-to-the-darknet-the-underground-for-the-underground/

Antonopoulos, A. M. (2015). *Mastering Bitcoin: Unlocking Digital Cryptocurrencies.* California: O'Reilly Media, Inc.

AskReddit. (2015, Dec 25). *Deep web users of reddit, what is the most fucked up/creepiest thing you've seen?* Ανάκτηση May 27, 2019, από AskReddit: https://www.reddit.com/r/AskReddit/comments/3y6nf3/deep_web_users_of_reddit_what_is_the_most_fucked/

Balduzzi, M., & Ciancaglini, V. (2015). *Cybercrime in the Deep Web.* Ανάκτηση May 25, 2019, από BlackHat: https://www.blackhat.com/docs/eu-15/materials/eu-15-Balduzzi-Cybercrmine-In-The-Deep-Web-wp.pdf

Barford, P., & Yegneswaran, V. (2007). An Inside Look at Botnets. Στο M. Christodorescu, S. Jha, D. Maughan, D. Song, & C. Wang, *Malware Detection* (σσ. 171-191). Boston, MA: Springer.

Batalla, J., Mastorakis, G., Mavromoustakis, C. X., & Pallis, E. (2017). *Beyond the Internet of Things: Everything Interconnected.* Switzerland: Springer International Publishing.

BBC. (2019, May 16). *What is the dark web and is it a threat?* Ανάκτηση από BBC - iWonder: http://www.bbc.co.uk/guides/z9j6nbk

Bergman, M. K. (2001, August). White Paper: The Deep Web: Surfacing Hidden Value. *Journal of Electronic Publishing (JEP), 7*(1). doi:10.3998/3336451.0007.104

Biryukov, A., Pustogarov, I., Thill, F., & Weinmann, R.-P. (2014). Content and popularity analysis of Tor hidden services. *IEEE Computer Society*, σσ. 188-193. Ανάκτηση από Cornell University: https://arxiv.org/pdf/1308.6768v2.pdf

Blank, A. G. (2002). *TCP/IP JumpStart: Internet Protocol Basics.* California: Sybex. Ανάκτηση από http://pacific.jour.auth.gr/totsidou/The_Internet.htm

Brandom, R. (2019, Feb 17). *The golden age of dark web drug markets is over.* Ανάκτηση May 29, 2019, από The Verge:

https://www.theverge.com/2019/2/17/18226718/alphabay-takedown-drug-marketplace-federal-arrest

Brantly, A. (2017). Innovation and Adaptation in Jihadist Digital Security. *Global Politics and Strategy, 59*(1), 79-102. doi:10.1080/00396338.2017.1282678

Carrington, K., Hogg, R., Scott, J., & Sozzo, M. (2018). *The Palgrave Handbook of Criminology and the Global South.* London: Palgrave Macmillan.

CERN. (2019). *The birth of the Web*. Retrieved May 06, 2019, from CERN: https://home.cern/science/computing/birth-web/short-history-web

Chen, H., Chung, W., Qin, J., Reid, E., Sageman, M., & Weimann, G. (2008, June). Uncovering the DarkWeb: A Case Study of Jihad. *Journal of the American Society for Information Science and Technology banner, 59*(8), pp. 1347-1359. doi:10.1002/asi.20838

Chertoff, M. (2017). A public policy perspective of the Dark Web. *Journal of Cyber Policy*, 26-38. doi:10.1080/23738871.2017.1298643

Ciancaglini, V., Balduzzi, M., Goncharov, M., & McArdle, R. (2013). *Deepweb and Cybercrime - It's Not All About TOR.* Ανάκτηση May 29, 2019, από Trend Micro Research: https://www.trendmicro.de/cloud-content/us/pdfs/security-intelligence/white-papers/wp-deepweb-and-cybercrime.pdf

Code, E. (2002). *Hackers Beware.* USA: New Riders Publishing.

Cox, J. (2015, January 11). *'Silk Road Reloaded' Just Launched on a Network More Secret than Tor.* Ανάκτηση May 29, 2019, από Tech by Vice: https://www.vice.com/en_us/article/wnj449/silk-road-reloaded-i2p

Crawley, A. (2016, September). Hiring hackers. *Network Security, 2016*(9), 13-15.

DeepWebLinks. (2019). *Is The Human Experiment on the Deep Web Really Exist?* Ανάκτηση May 29, 2019, από Deep Web Links: https://www.deepwebsiteslinks.com/the-human-experiment-on-the-deep-web-really-exist/

DeepWeb-Sites. (2019). *Deep Web Sites 2019 | Dark Web | Deep Web Links | Hidden Wiki.* Ανάκτηση από https://www.deepweb-sites.com

Desjardins, J. (2019, March 13). *What Happens in an Internet Minute in 2019?* Ανάκτηση May 25, 2019, από Visual Capitalist: https://www.visualcapitalist.com/what-happens-in-an-internet-minute-in-2019/

Dictionary.com. (2019). *Meanings and Definitions of Words.* Ανάκτηση May 13, 2019, από Dictionary.com: https://www.dictionary.com/

EC3. (2019). *Combating crime in a digital age.* Ανάκτηση June 1, 2019, από European Cybercrime Centre (EC3): https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3

EUGDPR. (2018). *GDPR Key Changes.* Ανάκτηση May 20, 2019, από EUGDPR: https://eugdpr.org/the-regulation/

European Commision. (2019, May 25). *GDPR In Numbers.* Ανάκτηση από European Commision: https://ec.europa.eu/commission/sites/beta-political/files/infographic-gdpr_in_numbers_1.pdf

Europol. (2019, March 26). *Global law enforcement action against vendors and buyers on the Dark Web.* Ανάκτηση από EUROPOL: https://www.europol.europa.eu/newsroom/news/global-law-enforcement-action-against-vendors-and-buyers-dark-web

Finklea, K. (2017, MArch 17). *Dark Web.* Ανάκτηση May 16, 2019, από Federation Of American Scientists: https://fas.org/sgp/crs/misc/R44101.pdf

Gamer, N. (2015, April 29). *What lies beneath: The deep web and future crimes.* Ανάκτηση από Trend Micro: https://blog.trendmicro.com/what-lies-beneath-the-deep-web-and-future-crimes/

Gehl, R. W. (2014). Power/freedom on the dark web: A digital ethnography of the Dark Web Social Network. *New Media & Society*, 1219-1235.

Gehl, R. W. (2018). *Weaving the Dark Web: Legitimacy on Freenet, Tor, and I2P.* London: The MIT Press.

Gomez, M. (2018, October 05). *Cryptocurrency Usage in Dark Web and Underground Markets: Cryptovest Investigates.* Ανάκτηση May 26, 2019, από CryptoVest: https://cryptovest.com/features/cryptocurrency-usage-in-dark-web-and-underground-markets-cryptovest-investigates/

Greenberg, A. (2013, November 18). *Meet The "Assassination Market" Creator Who's Crowdfunding Murder With Bitcoins.* Ανάκτηση May 27, 2019, από Forbes: https://www.forbes.com/sites/andygreenberg/2013/11/18/meet-the-assassination-market-creator-whos-crowdfunding-murder-with-bitcoins/

Greenberg, A. (2014, October 31). *Why Facebook Just Launched Its Own "Dark Web" Site.* Ανάκτηση May 16, 2019, από Wired.com: https://www.wired.com/2014/10/facebook-tor-dark-site/

Hsinchun, C. (2012). *Dark Web: Exploring and Data Mining the Dark Side of the Web.* London: Springer Science+Business Media.

ICANN. (2019, May 18). *Get-Started.* Ανάκτηση από ICANN: https://www.icann.org/get-started

Internet Society. (2019, May 10). *A Brief History of the Internet & Related Networks.* Retrieved from Internet Society: https://www.internetsociety.org/internet/history-internet/brief-history-internet-related-networks

Interpol. (2019, May 23). *50 children rescued, 9 sex offenders arrested in international operation.* Ανάκτηση May 30, 2019, από INTERPOL: https://www.interpol.int/en/News-and-Events/News/2019/50-children-rescued-9-sex-offenders-arrested-in-international-operation

Jewkes, Y., & Yar, M. (2010). *Handbook of Internet Crime.* Devon: Willan Publishing.

Kehoe, S. R. (2018, June 12). *The Digital Alleyway: Why the Dark Web Cannot Be Ignored.* Ανάκτηση May 30, 2019, από Police Chief Magazine: http://www.policechiefmagazine.org/the-digital-alleyway/

Kellmereit, D., & Obodovski, D. (2013). *The Silent Intelligence: The Internet of Things.* Minnesota: DND Ventures LLC.

Lautenschlager, S. (2016, April 22). *Surface Web, Deep Web, Dark Web -- What's the Difference?* Ανάκτηση May 13, 2019, από Cambia Research: https://www.cambiaresearch.com/articles/85/surface-web-deep-web-dark-web----whats-the-difference

Mohanta, A., Hahad, M., & Velmurugan, K. (2018). *Preventing Ransomware: Understand, prevent, and remediate ransomware attacks.* Birmingham: Packt Publishing.

Mueller, M. L. (2010). *Networks and States: The Global Politics of Internet Governance.* London: The MIT Press.

Murray, K. R., & Moen, W. E. (2015). The Deep Web: Resource Discovery in the Library of Texas. *Texas Library.*

Norry, A. (2018, November 20). *The History of Silk Road: A Tale of Drugs, Extortion & Bitcoin.* Ανάκτηση May 12, 2019, από Blockonomi.com: https://blockonomi.com/history-of-silk-road/

Ormsby, E. (2018). *The Darkest Web: Drugs, death and destroyed lives ... the inside story of the internet's evil twin.* Australia: Allen & Unwin.

Paganini, P. (2016, June 1). *Deep web illegal activity exceeds approximately $100,000,000.* Ανάκτηση May 27, 2019, από Security Affairs:

https://securityaffairs.co/wordpress/47904/cyber-crime/deep-web-cybercrime.html

Pederson, S. (2016). *Understanding the Deep Web in 10 Minutes.* Sioux Falls, USA: BrightPlanet.

Price, G., & Sherman, C. (2001). *The Invisible Web: Uncovering Information Sources Search Engines Can't See.* New Jersey: Information Today, Inc.

Routley, N. (2017, July 8). *The Dark Side of the Internet.* Ανάκτηση May 18, 2019, από Visual Capitalist: https://www.visualcapitalist.com/dark-web/

SOCTA. (2017). *Serious and Organised Crime Threat Assessment: Crime in the age of technology.* Ανάκτηση από European Union: https://www.europol.europa.eu/sites/default/files/documents/report_socta2017_1.pdf

Southwick, R. (2019). *Inside the dark web drug trade.* Ανάκτηση από CBC News: https://newsinteractives.cbc.ca/longform/the-new-frontier-of-the-drug-trade

STOP THE TRAFFIK. (2018). *Human Trafficking and the Darknet.* Ανάκτηση May 29, 2019, από STOP THE TRAFFIK: https://www.stopthetraffik.org/download/human-trafficking-darknet/?wpdmdl=11350

Strickland, J. (2008, March 3). *Who owns the Internet?* Ανάκτηση May 21, 2019, από How Stuff Works: https://computer.howstuffworks.com/internet/basics/who-owns-internet.htm

Stroukal, D., & Nedvědová, B. (2016). Bitcoin and other cryptocurrency as an instrument of crime in cyberspace. *Proceedings of the 4th Business & Management Conference.*

Sui, D., Caverlee, J., & Rudesill, D. (2015). The Deep Web and The Darknet: A look inside the internet's massive black box. *Wilson Center: Science + Technology Innovation Program.*

Territo, L., & Matteson, R. (2011). *The International Trafficking of Human Organs: A Multidisciplinary Perspective (Advances in Police Theory and Practice).* New York: CRC Press.

Tor Metrics. (2019, May 16). *Directly Connecting Relay Users.* Ανάκτηση από Tor Metrics: https://metrics.torproject.org/userstats-relay-country.html

Wardlaw, G. (1999, March). The future and crime: challenges for law enforcement. *Third National Outlook Symposium on Crime in Australia, Mapping the Boundaries of*

Australia's Criminal Justice System, convened by the Australian Institute of Criminology, Canberra, Australia.

Weimann, G. (2015). Terrorist Migration to the Dark Web. *Perspectives on Terrorism, 10*(3), 40-44.

WikiLeaks. (2015, November 03). *What is WikiLeaks.* Ανάκτηση May 16, 2019, από WikiLeaks: https://wikileaks.org

Zilman, M. P. (2019, May 1). *Deep Web Research and Discovery Resources 2019.* Ανάκτηση May 13, 2019, από Virtual Private Library: http://whitepapers.virtualprivatelibrary.net/DeepWeb.pdf

Zimmermann, K., & Emspak, J. (2017, June 27). *Internet History Timeline: ARPANET to the World Wide Web.* Ανάκτηση από Live Science: https://www.livescience.com/20727-internet-history.html

Αστυνομία Κύπρου. (2013, January 24). *Νέα περιστατικά στην Αστυνομία για απάτη μέσω διαδικτύου.* Ανάκτηση May 30, 2019, από ΑΣΤΥΝΟΜΙΑ ΚΥΠΡΟΥ: http://www.police.gov.cy/police/police.nsf/All/4843E9FD0FDA3094C2257AFD00327CCD/$file/Ast.%20Ana%CE%BA.%201.doc

Πανεπιστήμιο Θεσσαλίας. (1997, Δεκέμβριος). Ανάκτηση Μάϊος 05, 2019, από Η Ιστορία του Internet: http://www.uth.gr/main/help/help-desk/internet/internet3.html